aws

Benutzer-Leitfaden

Amazon Linux 2

Amazon Linux 2: Benutzer-Leitfaden

Table of Contents

Was ist Amazon Linux 2?

Amazon Linux 2 (AL2) ist ein Linux-Betriebssystem von Amazon Web Services (AWS). AL2 wurde entwickelt, um eine stabile, sichere und leistungsstarke Umgebung für Anwendungen bereitzustellen, die auf Amazon EC2 ausgeführt werden. Es enthält auch Pakete, die eine effiziente Integration ermöglichenAWS, darunter Startkonfigurationstools und viele beliebte AWS Bibliotheken und Tools. AWSbietet fortlaufende Sicherheits- und Wartungsupdates für alle laufenden Instances AL2. Viele Anwendungen, die auf CentOS und ähnlichen Distributionen entwickelt wurden, laufen auf. AL2 AL2 wird ohne zusätzliche Kosten zur Verfügung gestellt.

> **Note**
>
> AL2 ist nicht mehr die aktuelle Version von Amazon Linux. AL2023 ist der Nachfolger von. AL2 Weitere Informationen finden Sie unter AL2 Comparing and AL2 023 und in der Liste der Paketänderungen in AL2 023 im AL2023-Benutzerhandbuch.

> **Note**
>
> AL2 folgt der Upstream-Version von Firefox Extended Support Release (ESR) genau und aktualisiert auf die nächste ESR, sobald sie verfügbar ist. Weitere Informationen finden Sie im Firefox ESR-Veröffentlichungskalender und in den Versionshinweisen zu Firefox.

Amazon Linux-Verfügbarkeit

AWSbietet AL2 023, AL2, und Amazon Linux 1 (AL1früher Amazon Linux AMI). Wenn Sie von einer anderen Linux-Distribution zu Amazon Linux migrieren, empfehlen wir Ihnen, zu AL2 023 zu migrieren.

> **Note**
>
> Der Standardsupport für AL1 endete am 31. Dezember 2020. Die Phase des AL1 Wartungssupports endete am 31. Dezember 2023. Weitere Informationen zu AL1 EOL und Wartungssupport finden Sie im Blogbeitrag Update on Amazon Linux AMI end-of-life.

Weitere Informationen zu Amazon Linux finden Sie unter AL2023, AL2, und AL1.

Amazon-Linux-Container-Images finden Sie unter Amazon-Linux-Container-Image im Benutzerhandbuch für Amazon Elastic Container Registry.

Veraltete Funktionalität in AL2

In den folgenden Abschnitten werden Funktionen beschrieben, die in 023 unterstützt AL2 und nicht vorhanden sind. AL2 Dabei handelt es sich um Funktionen wie Funktionen und Pakete, die zwar in 023 vorhanden sind AL2, aber nicht in AL2 023 enthalten sind und auch nicht zu AL2 023 hinzugefügt werden. In der AL2 Dokumentation finden Sie Informationen darüber, wie lange diese Funktionalität unterstützt wird. AL2

`compat-`-Pakete

Alle Pakete AL2 mit dem Präfix von `compat-` werden aus Gründen der Binärkompatibilität mit älteren Binärdateien bereitgestellt, die noch nicht für moderne Versionen des Pakets neu erstellt wurden. Jede neue Hauptversion von Amazon Linux wird keine `compat-` Pakete aus früheren Versionen übernehmen.

Alle `compat-` Pakete in einer Version von Amazon Linux (z. B. AL2) sind nicht mehr verfügbar und in der nachfolgenden Version (z. B. AL2 023) nicht mehr enthalten. Wir empfehlen dringend, die Software anhand der aktualisierten Versionen der Bibliotheken neu zu erstellen.

Veraltete Funktionen wurden eingestellt in AL1, entfernt in AL2

In diesem Abschnitt werden Funktionen beschrieben, die in AL1 verfügbar sind und in nicht mehr verfügbar sind. AL2

> **Note**
>
> Im Rahmen der Wartungsunterstützungsphase von hatten einige Pakete ein end-of-life (EOL-) Datum AL1, das vor dem EOL von lag. AL1 Weitere Informationen finden Sie unter Erklärungen zur AL1 Paketunterstützung.

> **Note**
>
> Einige AL1 Funktionen wurden in früheren Versionen eingestellt. Informationen finden Sie in den AL1 Versionshinweisen.

Themen

32-Bit-x86 (i686) AMIs

Im Rahmen der Version 2014.09 von kündigte Amazon Linux an AL1, dass dies die letzte Version sein wird, die 32-Bit produziert. AMIs Daher unterstützt Amazon Linux ab Version 2015.03 von AL1 nicht mehr die Ausführung des Systems im 32-Bit-Modus. AL2 bietet eingeschränkte Laufzeitunterstützung für 32-Bit-Binärdateien auf x86-64-Hosts und stellt keine Entwicklungspakete zur Verfügung, die die Erstellung neuer 32-Bit-Binärdateien ermöglichen. AL2023 enthält keine 32-Bit-User-Space-Pakete mehr. Wir empfehlen Benutzern, die Umstellung auf 64-Bit-Code abzuschließen, bevor sie zu 023 migrieren. AL2

Wenn Sie 32-Bit-Binärdateien auf AL2 023 ausführen müssen, ist es möglich, den 32-Bit-Userspace AL2 innerhalb eines AL2 Containers zu verwenden, der auf 023 läuft. AL2

`aws-apitools-*`ersetzt durch AWS CLI

Vor der Veröffentlichung von AWS CLI im September 2013 wurde eine Reihe von Befehlszeilendienstprogrammen zur Verfügung AWS gestellt, die in implementiert wurden und es Benutzern ermöglichtenJava, EC2 Amazon-API-Aufrufe zu tätigen. Diese Tools wurden 2015 eingestellt und wurden zur AWS CLI bevorzugten Art, über die EC2 APIs Befehlszeile mit Amazon zu interagieren. Das Set an Befehlszeilen-Hilfsprogrammen umfasst die folgenden `aws-apitools-*` Pakete.

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

Der Upstream-Support für die `aws-apitools-*` Pakete endete im März 2017. Trotz des Mangels an Upstream-Unterstützung lieferte Amazon Linux weiterhin einige dieser Befehlszeilenprogramme

aus, z. B. `aws-apitools-ec2` um Benutzern Abwärtskompatibilität zu bieten. Das AWS CLI ist ein robusteres und vollständigeres Tool als die `aws-apitools-*` Pakete, da es aktiv gewartet wird und die Möglichkeit bietet, alle AWS APIs zu verwenden.

Die `aws-apitools-*` Pakete wurden im März 2017 als veraltet eingestuft und werden keine weiteren Updates erhalten. Alle Benutzer eines dieser Pakete sollten AWS CLI so schnell wie möglich auf das migrieren. Diese Pakete sind in AL2 023 nicht vorhanden.

AL1 hat auch die `aws-apitools-rds` Pakete `aws-apitools-iam` und bereitgestellt, die in AL1 Amazon Linux veraltet waren und ab AL2 jetzt nicht mehr in Amazon Linux vorhanden sind.

`systemd`ersetzt in **`upstart`** AL2

AL2 war die erste Amazon Linux-Version, die das `systemd` Init-System verwendete und `upstart` in AL1 ersetzte. Jede `upstart` spezifische Konfiguration muss im Rahmen der Migration von AL1 zu einer neueren Version von Amazon Linux geändert werden. Die Verwendung `systemd` auf ist nicht möglich AL1, daher `systemd` kann der Wechsel von `upstart` zu nur im Rahmen der Umstellung auf eine neuere Hauptversion von Amazon Linux wie AL2 or AL2 023 erfolgen.

Funktionalität wurde in 023 veraltet AL2 und wurde in Version 023 entfernt AL2

In diesem Abschnitt werden Funktionen beschrieben, die in 023 verfügbar und in AL2 Version 023 nicht mehr verfügbar sind. AL2

Themen

- 32-Bit-x86-Pakete (i686)
- aws-apitools-*ersetzt durch AWS CLI
- awslogsveraltet zugunsten eines vereinheitlichten Amazon CloudWatch Logs-Agenten
- bzrSystem zur Versionskontrolle
- cgroup v1
- log4jHotpatch () log4j-cve-2021-44228-hotpatch
- lsb_release und das system-lsb-core-Paket
- mcrypt
- OpenJDK (7) java-1.7.0-openjdk
- Python 2.7

- rsyslog-opensslersetzt rsyslog-gnutls
- Netzwerkinformationsdienst (NIS)/yp
- Mehrere Domainnamen in Amazon VPC create-dhcp-options
- Sun RPC in glibc
- OpenSSH-Schlüssel-Fingerabdruck im Protokoll audit
- ld.goldLinker
- ping6
- ftpPackage

32-Bit-x86-Pakete (i686)

Im Rahmen der Version 2014.09 von haben wir angekündigt AL1, dass dies die letzte Version sein wird, die 32-Bit-Version unterstützt. AMIs Daher unterstützt Amazon Linux ab Version 2015.03 von AL1 nicht mehr die Ausführung des Systems im 32-Bit-Modus. AL2 bietet eingeschränkte Laufzeitunterstützung für 32-Bit-Binärdateien auf x86-64-Hosts und stellt keine Entwicklungspakete zur Verfügung, um die Erstellung neuer 32-Bit-Binärdateien zu ermöglichen. AL2023 enthält keine 32-Bit-Userspace-Pakete mehr. Wir empfehlen Kunden, die Umstellung auf 64-Bit-Code abzuschließen.

Wenn Sie 32-Bit-Binärdateien auf AL2 023 ausführen müssen, ist es möglich, den 32-Bit-Userspace AL2 innerhalb eines AL2 Containers zu verwenden, der auf 023 läuft. AL2

`aws-apitools-*`ersetzt durch AWS CLI

Vor der Veröffentlichung von AWS CLI im September 2013 wurde eine Reihe von Befehlszeilendienstprogrammen zur Verfügung AWS gestellt, die in implementiert wurden und es Kunden ermöglichtenJava, EC2 Amazon-API-Aufrufe zu tätigen. Diese Tools wurden 2015 als veraltet eingestuft und wurden zur bevorzugten Art, über die Befehlszeile mit Amazon EC2 APIs zu interagieren. AWS CLI Dies beinhaltet die folgenden `aws-apitools-*` Pakete.

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

Der Upstream-Support für die `aws-apitools-*` Pakete endete im März 2017. Trotz des Mangels an Upstream-Unterstützung lieferte Amazon Linux weiterhin einige dieser Befehlszeilenprogramme (wie`aws-apitools-ec2`) aus, um Kunden Abwärtskompatibilität zu bieten. Das AWS CLI ist ein robusteres und vollständigeres Tool als die `aws-apitools-*` Pakete, da es aktiv gewartet wird und die Möglichkeit bietet, alle AWS APIs zu verwenden.

Die `aws-apitools-*` Pakete wurden im März 2017 als veraltet eingestuft und werden keine weiteren Updates erhalten. Alle Benutzer eines dieser Pakete sollten AWS CLI so schnell wie möglich auf das migrieren. Diese Pakete sind in AL2 023 nicht vorhanden.

`awslogs`veraltet zugunsten eines vereinheitlichten Amazon CloudWatch Logs-Agenten

Das `awslogs`Paket ist in 023 veraltet AL2 und ist in Version 023 nicht mehr vorhanden. AL2 Es wird durch den vereinheitlichten CloudWatch Logs-Agenten ersetzt, der im Paket verfügbar ist. `amazon-cloudwatch-agent` Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

`bzr`System zur Versionskontrolle

Das Revisionskontrollsystem GNU Bazaar(`bzr`) wurde in 023 eingestellt AL2 und ist seit AL2 023 nicht mehr verfügbar.

Benutzern von wird `bzr` empfohlen, ihre Repositorys zu zu migrieren. `git`

cgroup v1

AL2023 wechselt zur Unified Control Group-Hierarchie (cgroup v2), während cgroup v1 AL2 verwendet wird. Da cgroup v2 AL2 nicht unterstützt wird, muss diese Migration im Rahmen der Umstellung auf 023 abgeschlossen werden. AL2

log4jHotpatch () **`log4j-cve-2021-44228-hotpatch`**

> **Note**
>
> Das `log4j-cve-2021-44228-hotpatch` Paket ist in Version 023 veraltet AL2 und wurde in Version 023 entfernt. AL2

Als Reaktion auf CVE-2021-44228 veröffentlichte Amazon Linux eine RPM-Paketversion des Hotpatches für Apache Log4j für und. AL1 AL2 In der Ankündigung der Hinzufügung des Hotpatches zu Amazon Linux haben wir festgestellt, dass „die Installation des Hotpatches kein Ersatz für die Aktualisierung auf eine log4j-Version ist, die CVE-2021-44228 oder CVE-2021-45046 abmildert“.

Der Hotpatch diente lediglich als Abhilfemaßnahme, um mehr Zeit für den `log4j`-Patch zu gewinnen. Die erste allgemein verfügbare Version von AL2 023 wurde 15 Monate nach CVE-2021-44228 veröffentlicht, sodass 023 nicht mit dem Hotpatch ausgeliefert wird (aktiviert oder nicht). AL2

Kunden, die ihre eigenen `log4j`-Versionen auf Amazon Linux ausführen, sollten sicherstellen, dass sie auf Versionen aktualisiert haben, die nicht von CVE-2021-44228 oder CVE-2021-45046 betroffen sind.

`lsb_release` und das **`system-lsb-core`**-Paket

In der Vergangenheit rief manche Software den `lsb_release` Befehl (im `system-lsb-core` Paket enthalten) auf, um Informationen über die Linux-Distribution abzurufen, auf der sie ausgeführt AL2 wurde. Dieser Befehl wurde von Linux Standards Base (LSB) eingeführt und wurden von den Linux-Distributionen übernommen. Linux-Distributionen haben sich weiterentwickelt, sodass der einfachere Standard für die Speicherung dieser Informationen in `/etc/os-release` und anderen verwandten Dateien verwendet wird.

Der `os-release`-Standard stammt aus `systemd`. Weitere Informationen finden Sie in der systemd os-Versionsdokumentation.

AL2023 ist nicht im Lieferumfang des `lsb_release` Befehls enthalten und beinhaltet das `system-lsb-core` Paket nicht. Die Software sollte die Umstellung auf den `os-release`-Standard abschließen, um die Kompatibilität mit Amazon Linux und anderen wichtigen Linux-Distributionen aufrechtzuerhalten.

`mcrypt`

Die `mcrypt` Bibliothek und die zugehörige PHP Erweiterung waren in 023 veraltet und sind in AL2 023 nicht mehr vorhanden. AL2

Upstream PHP hat die `mcrypt` Erweiterung in PHP 7.1, die erstmals im Dezember 2016 veröffentlicht wurde und im Oktober 2019 endgültig veröffentlicht wurde, als veraltet eingestuft.

Die `mcrypt` Upstream-Bibliothek wurde zuletzt 2007 veröffentlicht und hat nicht die Migration von der `cvs` Versionskontrolle vorgenommen, die 2017 für neue Commits SourceForge erforderlich war. Der

letzte Commit (und nur für 3 Jahre davor) stammt aus dem Jahr 2011, wodurch die Erwähnung, dass das Projekt einen Betreuer hat, weggelassen wurde.

Allen verbleibenden Benutzern von wird `mcrypt` empfohlen, ihren Code auf 023 zu portierenOpenSSL, da dieser nicht zu AL2 023 hinzugefügt `mcrypt` wird.

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

> **Note**
>
> AL2023 bietet mehrere Versionen von Amazon Corretto zur Unterstützung Java von basierten Workloads. Die OpenJDK 7-Pakete sind in AL2 023 veraltet und nicht mehr vorhanden. AL2 Das älteste JDK, das in AL2 023 verfügbar war, wird von Corretto 8 bereitgestellt.

Weitere Informationen zu Java auf Amazon Linux finden Sie unterJavain AL2.

Python 2.7

> **Note**
>
> AL2023 hat Python 2.7 entfernt, sodass alle Betriebssystemkomponenten, die Python benötigen, so geschrieben sind, dass sie mit Python 3 funktionieren. Wenn Sie also weiterhin eine von Amazon Linux bereitgestellte und unterstützte Python-Version verwenden möchten, müssen Sie Ihren Python-2-Code in Python 3 konvertieren.

Weitere Informationen zu Python auf Amazon Linux finden Sie unterPythonin AL2.

`rsyslog-openssl`ersetzt **`rsyslog-gnutls`**

Das `rsyslog-gnutls` Paket ist in 023 veraltet und in AL2 Version 023 nicht mehr vorhanden. AL2 Das `rsyslog-openssl` Paket sollte ein direkter Ersatz für jegliche Nutzung des Pakets sein. `rsyslog-gnutls`

Netzwerkinformationsdienst (NIS)/**`yp`**

Der Network Information Service (NIS), ursprünglich Yellow Pages genannt oder in 023 nicht mehr unterstützt AL2, YP ist aber in 023 nicht mehr verfügbar. AL2 Dazu gehören die folgenden

Pakete:`ypbind`, und`ypserv`. `yp-tools` Bei anderen Paketen, die sich in integrieren NIS lassen, wurde diese Funktionalität in Version AL2 023 entfernt.

Mehrere Domainnamen in Amazon VPC `create-dhcp-options`

In Amazon Linux 2 war es möglich, mehrere Domainnamen im `domain-name` Parameter an zu übergeben `create-dhcp-options`, was dazu führen würde, dass sie etwas wie `/etc/resolv.conf` enthalten würden`search foo.example.com bar.example.com`. Der Amazon DHCP VPC-Server sendet die Liste der bereitgestellten Domainnamen mit DHCP Option 15, die nur einen einzelnen Domainnamen unterstützt (siehe RFC 2132, Abschnitt 3.17). Da AL2 023 `systemd-networkd` für die Netzwerkkonfiguration verwendet wird, was auf die folgtRFC, ist diese zufällige Funktion in AL2 023 nicht vorhanden AL2

In der AWS CLIDokumentation von Amazon VPC heißt es dazu: „Einige Linux-Betriebssysteme akzeptieren mehrere durch Leerzeichen getrennte Domainnamen. Andere Linux-Betriebssysteme behandeln den Wert jedoch als eine einzelne Domain, was zu unerwartetem Verhalten führt. Windows Wenn Ihr DHCP Optionssatz mit einer Amazon-VPC verknüpft ist, deren Instances Betriebssysteme ausführen, die den Wert als einzelne Domain behandeln, geben Sie nur einen Domainnamen an. “

Auf diesen Systemen, z. B. AL2 023, werden zwei Domänen mit der DHCP Option 15 angegeben (die nur eine erlaubt), und da das Leerzeichen in Domainnamen ungültig ist, führt dies dazu, dass das Leerzeichen als codiert wird`032`, was zu enthält führt. `/etc/resolv.conf search foo.exmple.com032bar.example.com`

Um mehrere Domainnamen zu unterstützen, sollte ein DHCP Server DHCP Option 119 verwenden (siehe RFC 3397, Abschnitt 2). Im Amazon VPC-Benutzerhandbuch erfahren Sie, wann dies vom Amazon DHCP VPC-Server unterstützt wird.

Sun RPC in `glibc`

Die Implementierung von Sun RPC in `glibc` ist in Version 023 veraltet und wurde in AL2 Version 023 entfernt. AL2 Kunden wird empfohlen, zur Verwendung der `libtirpc` Bibliothek (verfügbar in AL2 und AL2 023) überzugehen, falls Sun RPC Funktionen erforderlich sind. Die Einführung ermöglicht `libtirpc` auch die Unterstützung IPv6 von Anwendungen.

Diese Änderung spiegelt die allgemeine Akzeptanz der Upstream-Version wider, diese Funktionalität zu `glibc` entfernen, zum Beispiel die Entfernung von Sun RPC Schnittstellen aus `glibc` Fedora und eine ähnliche Änderung in Gentoo.

OpenSSH-Schlüssel-Fingerabdruck im Protokoll **audit**

Später im Lebenszyklus von wurde dem OpenSSH-Paket ein Patch hinzugefügt AL2, der den zur Authentifizierung verwendeten Schlüsselfingerabdruck ausgibt. Diese Funktionalität ist in 023 nicht vorhanden. AL2

ld.gold Linker

Der `ld.gold` Linker ist in 023 verfügbar und wird in AL2 023 entfernt. AL2 Kunden, die Software entwickeln, die explizit auf den gold Linker verweist, sollten auf den regulären Linker () `ld.bfd` migrieren.

Die Upstream-Versionshinweise zu GNU Binutils für Version 2.44 (veröffentlicht im Februar 2025) dokumentieren die Entfernung von`ld.gold`: „In einer Änderung unserer bisherigen Praxis enthält der binutils-2.44.tar-Tarball in dieser Version nicht die Quellen für den Gold-Linker. Das liegt daran, dass der Gold-Linker nun veraltet ist und irgendwann entfernt werden wird, sofern sich nicht Freiwillige melden und anbieten, die Weiterentwicklung und Wartung fortzusetzen.“

ping6

In AL2 023 unterstützt das reguläre `ping` Hilfsprogramm nativ IPv6, und das separate Programm `/bin/ping6` ist nicht mehr erforderlich. In AL2 023 `/usr/sbin/ping6` ist es ein Symlink zur ausführbaren Datei. `/usr/bin/ping`

Diese Änderung folgt auf die Einführung neuerer `iputils` Versionen, die diese Funktionalität bieten, durch die breitere Community, beispielsweise die IPv6 Ping-Änderung in Fedora.

ftpPackage

Das `ftp` Paket in AL2 ist ab AL2 023 nicht mehr in Amazon Linux verfügbar. Diese Entscheidung wurde im Rahmen unseres kontinuierlichen Engagements für Sicherheit, Wartbarkeit und moderne Softwareentwicklungspraktiken getroffen. Im Rahmen der (oder davor) Migration auf Version AL2 023 empfehlen wir, jegliche Verwendung des `ftp` Legacy-Pakets auf eine seiner Alternativen zu migrieren.

Hintergrund

Das `ftp` Legacy-Paket wurde im Upstream-Bereich seit vielen Jahren nicht mehr aktiv gepflegt. Die letzte bedeutende Aktualisierung des Quellcodes erfolgte Anfang der 2000er Jahre, und das

ursprüngliche Quell-Repository ist nicht mehr verfügbar. Während einige Linux-Distributionen Patches für Sicherheitslücken enthielten, ist die Codebasis nach wie vor weitgehend unbewirtschaftet.

Empfohlene Alternativen

AL2023 bietet mehrere moderne, aktiv gepflegte Alternativen für FTP-Funktionen:

`lftp`(verfügbar in AL2 und AL2 023)

Ein ausgeklügeltes Dateiübertragungsprogramm, das FTP, HTTP, SFTP und andere Protokolle unterstützt. Es bietet mehr Funktionen als der herkömmliche `ftp` Client und wird aktiv gewartet.

Installiere mit: dnf install lftp

`curl`(verfügbar in AL2 und AL2 023)

Ein vielseitiges Befehlszeilentool für die Übertragung von Daten mit URLs Unterstützung von FTP, FTPS, HTTP, HTTPS und vielen anderen Protokollen.

Standardmäßig in AL2 023 über das Paket verfügbar. `curl-minimal` Für eine umfassendere Protokollunterstützung können Sie optional ein Upgrade auf die `curl-full` Verwendung vondnf swap curl-minimal curl-full.

`wget`(verfügbar in AL2 und AL2 023)

Ein nicht interaktives Befehlszeilenprogramm zum Herunterladen von Dateien aus dem Internet, das die Protokolle HTTP, HTTPS und FTP unterstützt.

Installation mit: dnf install wget (standardmäßig nicht in allen AL2 023 Images installiert)

`sftp`(verfügbar in AL2 und AL2 023)

Ein sicheres Dateiübertragungsprotokoll, das über SSH funktioniert und verschlüsselte Dateiübertragungen ermöglicht.

Standardmäßig als Teil des OpenSSH-Pakets verfügbar.

Überlegungen zur Migration

Wenn Ihre Anwendungen oder Skripts vom `ftp` Legacy-Client abhängen, sollten Sie die folgenden Migrationsansätze in Betracht ziehen:

1. Aktualisieren Sie Skripts, um moderne Alternativen zu verwenden: Ändern Sie Ihre Skripts so`lftp`,,`curl`,`wget`, oder `sftp` anstelle des `ftp` Legacy-Clients zu verwenden.

2. Überprüfen Sie die Paketabhängigkeiten: Einige Anwendungen führen das `ftp` Paket möglicherweise als Abhängigkeit in ihren Paketmetadaten auf, obwohl sie seit langem intern auf die Verwendung moderner Protokolle umgestellt haben. In diesen Fällen kann es sein, dass die Anwendung auf AL2 023 korrekt funktioniert, obwohl sie nicht im Paket `/usr/bin/ftp` enthalten ist`ftp`. Prüfen Sie die tatsächlichen Anforderungen Ihrer Anwendung, anstatt sich ausschließlich auf die angegebenen Abhängigkeiten zu verlassen.
3. Aktualisieren Sie die Anwendungsabhängigkeiten: Bei Anwendungen, die Sie verwalten und die zwar immer noch eine Abhängigkeit vom `ftp` Paket deklarieren, es aber nicht wirklich verwenden, aktualisieren Sie die Paketmetadaten, um diese unnötige Abhängigkeit zu entfernen.

Sicherheitsüberlegungen

Das FTP-Protokoll überträgt Daten, einschließlich Anmeldeinformationen, im Klartext. Für sicherheitsrelevante Anwendungen empfehlen wir dringend, verschlüsselte Alternativen wie SFTP oder HTTPS zu verwenden, die von den empfohlenen alternativen Tools unterstützt werden.

Bereiten Sie Ihre Migration auf AL2 023 vor

Sie können Ihren Umstieg auf AL2 023 vorbereiten, während Sie es weiterhin verwenden. AL2

Themen

Sehen Sie sich die Liste der Änderungen in 023 an AL2

Die AL2 023-Dokumentation enthält eine detaillierte Liste der Änderungen, die seitdem implementiert wurden. AL2 Diese Informationen befinden sich im Abschnitt Vergleichen AL2 und AL2 023.
Eine umfassende Liste der Änderungen an Softwarepaketen finden Sie auch im Abschnitt Paketänderungen in AL2 023.

AL2023 beinhaltet nicht. `amazon-linux-extras` Stattdessen stellt es Pakete mit Namespaces bereit, in denen mehrere Versionen bereitgestellt werden. Da viele Pakete in AL2 023 aktualisiert werden, sind die Basisversionen in AL2 023 möglicherweise später als die Versionen, aus denen Sie sie beziehen. `amazon-linux-extras`

> **Note**
>
> Wir empfehlen, dass Sie das Programm nicht ausführen`amazon-linux-extras`, da es EOL ist.

Nachdem Sie diese Abschnitte in der Dokumentation gelesen haben, können Sie feststellen, ob es Änderungen in AL2 023 gibt, aufgrund derer Sie Ihre Umgebung möglicherweise an die Migration anpassen müssen. Beispielsweise müssen Sie möglicherweise endlich ein Python 2.7-Skript auf Python 3 migrieren.

Migrieren Sie von **`systemd`** Jobs zu Timern **`cron`**

Standardmäßig `cron` ist in AL2 023 nicht installiert. Sie können Ihre `cron` Jobs in Vorbereitung auf die Migration zu 023 AL2 auf `systemd` Timer migrieren. AL2 `systemd`bietet viele Vorteile,

wie z. B. eine genauere Kontrolle darüber, wann Timer ausgeführt werden, und eine verbesserte Protokollierung.

AL2 Einschränkungen

Die folgenden Themen behandeln verschiedene Einschränkungen von AL2 und ob sie in einer neueren Version von Amazon Linux behoben wurden.

Themen

yumkann GPG-Signaturen, die mit GPG-Unterschlüsseln erstellt wurden, nicht verifizieren

Die Version des `rpm` Paketmanagers AL2 ist von früher und `rpm` hat Unterstützung für die Überprüfung von Paketsignaturen hinzugefügt, die mit GPG-Unterschlüsseln erstellt wurden. Wenn Sie Pakete erstellen AL2, mit denen kompatibel sein soll, müssen Sie sicherstellen, dass Sie GPG-Signaturschlüssel verwenden, die mit dem`rpm`, was Teil von ist, kompatibel sind AL2

Um die Abwärtskompatibilität für bestehende Benutzer zu gewährleisten, AL2 erhält die Version von `rpm` in nur Sicherheits-Backports.

Die Version von `rpm` in AL2 023 unterstützt die Überprüfung von Paketsignaturen, die mit GPG-Unterschlüsseln erstellt wurden.

Vergleiche AL1 und AL2

In den folgenden Themen werden die wichtigsten Unterschiede zwischen AL1 und beschrieben AL2. Sie enthalten auch Informationen zur Lebensdauer und zum Support sowie zu Paketänderungen.

Themen

AL1 Support und EOL

AL1 ist jetzt EOL. AL1 beendete den Standardsupport am 31. Dezember 2020 und befand sich bis zum 31. Dezember 2023 in einer Wartungssupportphase.

Wir empfehlen ein Upgrade auf die neueste Amazon Linux-Version.

Support für AWS Graviton-Prozessoren

AL2 hat Unterstützung für Graviton-Prozessoren eingeführt. AL2023 ist weiter für Graviton-Prozessoren optimiert.

`systemd` ersetzt **`upstart`** als **`init`**-System

In AL2, `systemd` ersetzt `upstart` als das `init` System.

Python 2.6 und 2.7 wurden durch Python 3 ersetzt

Obwohl Python 2.6 mit der Version 2018.03 als EOL AL1 markiert wurde, befanden sich die Pakete immer noch in den zu installierenden Repositorys. AL2 wurde mit Python 2.7 als frühester unterstützter Python-Version ausgeliefert.

AL2023 schließt den Übergang zu Python 3 ab, und es sind keine Python 2.x-Versionen in den Repositorys enthalten.

Vergleichen von Paketen, die auf AL1 und installiert sind 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-Erweiterung		2.0.3
amazon-ssm-agent	3.2.1705.0	3.2.1705.0
at	3.1.10	3.1.13
attr	2.4.46	2,4,46
audit	2.6.5	2.8.1
audit-libs	2.6.5	2.8.1
authconfig	6.2.8	6.2.8
aws-amitools-ec2	1.5.13	
aws-cfn-bootstrap	1.4	2.0
aws-cli	1.18,107	

Package	AL1 AMI	AL2 AMI
awscli		1.18,147
basesystem	10.0	10.0
bash	4.2,46	4.2,46
bash-completion		2.1
bc	1,06,95	1,06,95
bind-export-libs		9,11,4
bind-libs	9.8.2	9.11,4
bind-libs-lite		9.11,4
bind-license		9.11,4
bind-utils	9.8.2	9.11,4
binutils	2,27	2,29,1
blktrace		1.0.5
boost-date-time		1,53,0
boost-system		1,53,0
boost-thread		1,53,0
bridge-utils		1.5
bzip2	1.0.6	1.0.6
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023,2,62	2023,2,62
checkpolicy	2.1.10	

Package	AL1 AMI	AL2 AMI
chkconfig	1.3.49,3	1.7.4
chrony		4.2
cloud-disk-utils	0,27	
cloud-init	0,7.6	19,3
cloud-utils-growpart		0,31
copy-jdk-configs	3,3	
coreutils	8,22	8,22
cpio	(2.10)	2.12
cracklib	2.8,16	2.9.0
cracklib-dicts	2.8,16	2.9.0
cronie	1.4.4	1.4.11
cronie-anacron	1.4.4	1.4.11
crontabs	1.10	1.11
cryptsetup	1.6.7	1.7.4
cryptsetup-libs	1.6.7	1.7.4
curl	7,61,1	8.3,0
cyrus-sasl	2.1.23	
cyrus-sasl-lib	2.1.23	2.1.26
cyrus-sasl-plain	2.1.23	2.1.26
dash	0.5.5.1	

Package	AL1 AMI	AL2 AMI
db4	4.7.25	
db4-utils	4,7,25	
dbus	1.6.12	1.10.24
dbus-libs	1.6.12	1.10.24
dejavu-fonts-common	2,33	
dejavu-sans-fonts	2,33	
dejavu-serif-fonts	2,33	
device-mapper	1,02,135	1,02,170
device-mapper-event	1,02,135	1,02,170
device-mapper-event-libs	1,02,135	1,02,170
device-mapper-libs	1,02,135	1,02,170
device-mapper-persistent-data	0,6.3	0.7.3
dhclient	4.1.1	4.2.5
dhcp-common	4.1.1	4.2.5
dhcp-libs		4.2.5
diffutils	3.3	3.3
dmidecode		3.2
dmraid	1.0.0.rc16	1.0.0.rc16
dmraid-events	1.0.0.rc16	1.0.0.rc16
dosfstools		3.0.20

Package	AL1 AMI	AL2 AMI
dracut	004	033
dracut-config-ec2		2.0
dracut-config-generic		033
dracut-modules-growroot	0.20	
dump	0.4	
dyninst		9.3.1
e2fsprogs	1.43,5	1,42,9
e2fsprogs-libs	1.43,5	1,42,9
ec2-hibinit-agent	1.0.0	1.0.2
ec2-instance-connect		1.1
ec-2 instance-connect-selinux		1.1
ec2-net-utils	0.7	1.7.3
ec2-utils	0.7	1.2
ed	1.1	1.9
elfutils-default-yama-scope		0,176
elfutils-libelf	0,168	0,176
elfutils-libs		0,176
epel-release	6	
ethtool	3,15	4,8
expat	2.1.0	2.1.0

Package	AL1 AMI	AL2 AMI
file	5,37	5,11
file-libs	5,37	5,11
filesystem	2,4,30	3.2
findutils	4.4.2	4.5.11
fipscheck	1.3.1	1.4.1
fipscheck-lib	1.3.1	1.4.1
fontconfig	2.8.0	
fontpackages-filesystem	1,41	
freetype	2.3.11	2.8
fuse-libs	2.9.4	2.9.2
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
gdisk	0.8.10	0,8,10
generic-logos	17.0.0	18.0.0
get_reference_source	1.2	
gettext		0.19.8.1
gettext-libs		0.19.8.1
giflib	4.1.6	
glib2	2,36,3	2,56,1
glibc	2,17	2,26

Package	AL1 AMI	AL2 AMI
glibc-all-langpacks		2,26
glibc-common	2,17	2,26
glibc-locale-source		2,26
glibc-minimal-langpack		2,26
gmp	6.0.0	6.0.0
gnupg2	2.0.28	2.0.22
gpgme	1.4.3	1.3.2
gpm-libs	1,20,6	1,20,7
grep	2,20	2,20
groff	1,22,2	
groff-base	1.22.2	1.22.2
grub	0,97	
grub2		2,06
grub2-common		2,06
grub2-efi-x64-ec2		2,06
grub2-pc		2,06
grub2-pc-modules		2,06
grub2-tools		2,06
grub2-tools-minimal		2,06
grubby	7,0,15	8,28

Package	AL1 AMI	AL2 AMI
gssproxy		0.7.0
gzip	1.5	1.5
hardlink		1.3
hesiod	3.1.0	
hibagent	1.0.0	1.1.0
hmaccalc	0,9,12	
hostname		3.13
hunspell		1.3.2
hunspell-en		0,20121024
hunspell-en-GB		0,20121024
hunspell-en-US		0,20121024
hwdata	0,233	0,252
info	5.1	5.1
initscripts	9,03,58	9,49,47
iproute	4.4.0	5.10.0
iptables	1,4,21	1.8.4
iptables-libs		1.8.4
iputils	20121221	20180629
irqbalance	1.5.0	1.7.0
jansson		(2.10)

Package	AL1 AMI	AL2 AMI
java-1.7.0-openjdk	1.7.0.321	
javapackages-tools	0.9.1	
jbigkit-libs		2.0
jpackage-utils	1.7.5	
json-c		0,11
kbd	1.15	1,1,5
kbd-legacy		1,1,5
kbd-misc	1.15	1,1,5
kernel	4,14.326	5.10,199
kernel-tools	4,14.326	5.10,199
keyutils	1.5.8	1.5.8
keyutils-libs	1.5.8	1.5.8
kmod	14	25
kmod-libs	14	25
kpartx	0.4.9	0,4.9
kpatch-runtime		0.9.4
krb5-libs	1.15.1	1.15.1
langtable		0.0.31
langtable-data		0.0.31
langtable-python		0.0.31

Package	AL1 AMI	AL2 AMI
lcms2	2.6	
less	436	458
libICE	1.0.6	
libSM	1.2.1	
libX11	1.6.0	
libX11-common	1.6.0	
libXau	1.0.6	
libXcomposite	0,4,3	
libXext	1.3.2	
libXfont	1.4.5	
libXi	1.7.2	
libXrender	0.9.8	
libXtst	1.2.2	
libacl	2,2,49	2,2,51
libaio	0,3.109	0,3.109
libassuan	2.0.3	2.1.0
libattr	2,4,46	2,4,46
libbasicobjects		0.1.1
libblkid	2,23,2	2,30,2
libcap	2,16	2,54

Package	AL1 AMI	AL2 AMI
libcap-ng	0,7,5	0.7.5
libcap54	2,54	
libcgroup	0,40 %rc1	
libcollection		0.7.0
libcom_err	1,43,5	1,42,9
libconfig		1.4.9
libcroco		0.6.12
libcrypt		2,26
libcurl	7,61,1	8.3,0
libdaemon		0,14
libdb		5.3.21
libdb-utils		5.3.21
libdrm		2,4,97
libdwarf		20130207
libedit	2.11	3.0
libestr		0,19
libevent	2.0.21	2.0.21
libfastjson		0,99,4
libfdisk		2,30,2
libffi	3.0,13	3.0,13

Package	AL1 AMI	AL2 AMI
libfontenc	1.0.5	
libgcc		7.3.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgomp		7.3.1
libgpg-error	1.11	1.12
libgssglue	0.1	
libicu	50,2	50,2
libidn	1,18	1,28
libidn2	2.3.0	2.3.0
libini_config		1.3.1
libjpeg-turbo	1,2,90	2,0,90
libmetalink		0.1.3
libmnl	1.0.3	1.0.3
libmount	2,23,2	2,30,2
libnetfilter_conntrack	1.0.4	1.0.6
libnfnetlink	1.0.1	1.0.1
libnfsidmap	0,25	0,25
libnghttp2	1,33,0	1,41,0
libnih	1.0.1	

Package	AL1 AMI	AL2 AMI
libnl	1.1.4	
libnl3		3.2,28
libnl3-cli		3.2.28
libpath_utils		0.2.1
libpcap		1.5.3
libpciaccess		0,14
libpipeline	1.2.3	1.2.3
libpng	1,2,49	1.5.13
libpsl	0.6.2	
libpwquality	1.2.3	1.2.3
libref_array		0.1.5
libseccomp		2.4.1
libselinux	2.1.10	2.5
libselinux-utils	2.1.10	2.5
libsemanage	2.1.6	2.5
libsepol	2.1.7	2.5
libsmartcols	2,23,2	2,30,2
libss	1,43,5	1,42,9
libssh2	1.4.2	1.4.3
libsss_idmap		1.16,5

Package	AL1 AMI	AL2 AMI
libsss_nss_idmap		1,16,5
libstdc++		7.3.1
libstdc++72	7.2.1	
libstoragemgmt		1.6.1
libstoragemgmt-python		1.6.1
libstoragemgmt-python-clibs		1.6.1
libsysfs	2.1.0	2.1.0
libtasn1	2.3	4,10
libteam		1,27
libtiff		4.0.3
libtirpc	0.2.4	0.2.4
libudev	173	
libunistring	0.9.3	0.9.3
libuser	0,60	0,60
libutempter	1.1.5	1.1.6
libuuid	2,23,2	2,30,2
libverto	0,2,5	0,2,5
libverto-libevent		0,2,5
libwebp		0.3.0
libxcb	1.11	

Package	AL1 AMI	AL2 AMI
libxml2	2.9.1	2.9.1
libxml2-python		2.9.1
libxml2-python27	2.9.1	
libxslt	1.1.28	
libyaml	0.1.6	0.1.4
lm_sensors-libs		3.4.0
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3.7.8	3.8.6
lsof	4,82	4,87
lua	5.1.4	5.1.4
lvm2	2.02.166	2.02.187
lvm2-libs	2.02.166	2.02.187
lz4		1.7.5
mailcap	2.1.31	
make	3,82	3,82
man-db	2.6.3	2.6.3
man-pages	4,10	3,53
man-pages-overrides		7.5.2
mariadb-libs		5.5,68
mdadm	3.2.6	4,0

Package	AL1 AMI	AL2 AMI
microcode_ctl	2.1	2.1
mingetty	1,08	
mlocate		0,26
mtr		0.92
nano	2.5.3	2,9,8
nc	1,84	
ncurses	5,7	6.0
ncurses-base	5,7	6.0
ncurses-libs	5,7	6.0
net-tools	1,60	2.0
nettle		2.7.1
newt	0,52,11	0,52,15
newt-python		0,52,15
newt-python27	0,52,11	
nfs-utils	1.3.0	1.3.0
nspr	4,25,0	4,35,0
nss	3,53,1	3,90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3,53,1	3,90,0
nss-softokn-freebl	3,53,1	3,90,0

Package	AL1 AMI	AL2 AMI
nss-sysinit	3,53,1	3,90,0
nss-tools	3,53,1	3,90,0
nss-util	3,53,1	3,90,0
ntp	4.2.8 p 15	
ntpdate	4.2.8p15	
ntsysv	1.3.49,3	1.7.4
numactl	2.0.7	
numactl-libs		2.0.9
OpenLDAP	2,4,40	2,4,44
openssh	7.4p1	7,4p1
openssh-clients	7,4p1	7,4p1
openssh-server	7,4p1	7,4p1
OpenSSL	1,2k	1,02 k
openssl-libs		1,02 k
os-prober		1.58
p11-kit	0,18,5	0,23,22
p11-kit-trust	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	
parted	2.1	3.1
passwd	0,79	0,79
pciutils	3,10	3.5.1
pciutils-libs	3.1.10	3.5.1
pcre	8,21	8,32
pcre2		10,23
perl	5,16.3	5.16.3
perl-Carp	1,26	1,26
perl-Digest	1,17	
perl-Digest-HMAC	1,03	
Perl-Digest- MD5	2,52	
perl-Digest-SHA	5,85	
perl-Encode	2,51	2,51
perl-Exporter	5,68	5,68
perl-File-Path	2,09	2,09
perl-File-Temp	0,23,01	0,23,01
perl-Filter	1,49	1,49
perl-Getopt-Long	2,40	2,40
perl-HTTP-Tiny	0,033	0,033

Package	AL1 AMI	AL2 AMI
Perl- PathTools	3,40	3,40
perl-Pod-Escapes	1.04	1.04
perl-Pod-Perldoc	3,20	3,20
perl-Pod-Simple	3,28	3,28
perl-Pod-Usage	1,63	1,63
perl-Scalar-List-Utils	1,27	1,27
perl-Socket	2,010	2,010
perl-Storable	2,45	2,45
Perl-Text- ParseWords	3,29	3,29
Perl-Zeit- HiRes	1,9725	1,9725
perl-Time-Local	1,2300	1,2300
perl-constant	1,27	1,27
perl-libs	5,16.3	5.16.3
perl-macros	5.16.3	5.16.3
perl-parent	0,225	0,225
perl-podlators	2.5.1	2.5.1
perl-threads	1,87	1,87
perl-threads-shared	1,43	1,43
pinentry	0,7.6	0.8.1
pkgconfig	0,27,1	0,27,1

Package	AL1 AMI	AL2 AMI
plymouth		0,8,9
plymouth-core-libs		0,8,9
plymouth-scripts		0,8,9
pm-utils	1.4.1	1.4.1
policycoreutils	2.1.12	2.5
popt	1.13	1.13
postfix		2.10.1
procmail	3,22	
procps	3.2.8	
procps-ng		3.3.10
psacct	6.3.2	6.6.1
psmisc	22,20	22,20
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0,5.3
pystache		0,5.3
python		2.7.18
python-babel		0.9.6
python-backports		1,0
python-backports-ssl_überei nstimmender_Hostname		3.5.0.1

Package	AL1 AMI	AL2 AMI
python-cffi		1.6.0
python-chardet		2.2.1
python-configobj		4.7.2
python-daemon		1,6
python-devel		2.7.18
python-docutils		0,12
python-enum34		1.0.4
python-idna		2.4
python-iniparse		0.4
python-ipaddress		1.0.16
python-jinja2		2.7.2
python-jsonpatch		1.2
python-jsonpointer		1.9
python-jwcrypto		0.4.2
python-kitchen		1.1.1
python-libs		2.7.18
python-lockfile		0.9.1
python-markupsafe		0,11
python-pillow		2.0.0
python-ply		3.4

Package	AL1 AMI	AL2 AMI
python-pycparser		2.14
python-pycurl		7,19,0
python-repoze-lru		0.4
python-requests		2.6.0
python-simplejson		3.2.0
python-urlgrabber		3,10
python-urllib3		1,25,9
python2-botocore		1.18,6
python2-colorama		0.3.9
python2-cryptography		1.7.2
python2-dateutil		2.6.1
python2-futures		3.0.5
python2-jmespath		0.9.3
python2-jsonschema		2.5.1
python2-oauthlib		2.0.1
python2-pyasn1		0.1.9
python2-rpm		4.11.3
python2-rsa		3.4.1
python2-s3transfer		0.3.3
python2-setuptools		41,2,0

Package	AL1 AMI	AL2 AMI
python2-six		1.11.0
python27	2.7.18	
python27-PyYAML	3,10	
python27-babel	0.9.4	
python27-backports	1,0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-boto	2,48,0	
python27-botocore	1,17,31	
python27-chardet	2.0.1	
python27-colorama	0.4.1	
python27-configobj	4.7.2	
python27-crypto	2.6.1	
python27-daemon	1.5.2	
python27-dateutil	2.1	
python27-devel	2.7.18	
python27-docutils	0,11	
python27-ecdsa	0,11	
python27-futures	3.0.3	
python27-imaging	1.1.6	
python27-iniparse	0.3.1	

Package	AL1 AMI	AL2 AMI
python27-jinja2	2.7.2	
python27-jmespath	0.9.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1,0	
python27-kitchen	1.1.1	
python27-libs	2.7.18	
python27-lockfile	0.8	
python27-markupsafe	0,11	
python27-paramiko	1.15.1	
python27-pip	9.0.3	
python27-ply	3.4	
python27-pyasn1	0.1.7	
python27-pycurl	7.19.0	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	
python27-pystache	0,5.3	
python27-pyxattr	0.5.0	
python27-requests	1.2.3	
python27-rsa	3.4.1	
python27-setuptools	36,2,7	

Package	AL1 AMI	AL2 AMI
python27-simplejson	3.6.5	
python27-six	1.8.0	
python27-urlgrabber	3,10	
python27-urllib3	1,24,3	
python27-virtualenv	15.1,0	
python3		3.7.16
python3-daemon		2.2.3
python3-docutils		0,14
python3-libs		3.7,16
python3-lockfile		0.11.0
python3-pip		20.2.2
python3-pystache		0.5.4
python3-setuptools		491,3
python3-simplejson		3.2.0
pyxattr		0.5.1
qrencode-libs		3.4.1
quota	4,00	4,01
quota-nls	4,00	4,01
rdate		1.4
readline	6.2	6.2

Package	AL1 AMI	AL2 AMI
rmt	0.4	
rng-tools	5	6.8
rootfiles	8,1	8.1
rpcbind	0.2.0	0.2.0
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-plugin-systemd-inhibit		4.11.3
rpm-python27	4.11.3	
rsync	3.0.6	3.1.2
rsyslog	5.8.10	8,24,0
ruby	2.0	
ruby20	2.0.0.648	
ruby20-irb	2.0.0.648	
ruby20-libs	2.0.0.648	
rubygem20-bigdecimal	1.2.0	
rubygem20-json	1.8.3	
rubygem20-psych	2.0.0	
rubygem20-rdoc	4.2.2	
rubygems20	2.0.14.1	

Package	AL1 AMI	AL2 AMI
scl-utils		20130529
screen	4.0.3	4.1.0
sed	4.2.1	4.2.2
selinux-policy		3.13.1
selinux-policy-targeted		3.13,1
sendmail	8.14,4	
setserial	2,17	2,17
Einrichten	2.8,14	2,8,71
setuptool		1.19,11
sgpio	1.2.0.10	1.2.0.10
shadow-utils	4.1.4.2	4.1.5.1
shared-mime-info	1.1	1.8
slang	2.2.1	2.2.4
sqlite	3.7.17	3.7.17
sssd-client		1.16,5
strace		4,26
sudo	1,8,23	1,8,23
sysctl-defaults	1,0	1,0
sysfsutils	2.1.0	
sysstat		10.1.5

Package	AL1 AMI	AL2 AMI
system-release	2018,03	2
systemd		219
systemd-libs		219
systemd-sysv		219
systemtap-runtime		4,5
sysvinit	2,87	
sysvinit-tools		2,88
tar	1,26	1,26
tcp_wrappers	7.6	7.6
tcp_wrappers-libs	7.6	7.6
tcpdump		4.9.2
tcsh		6,18,01
teamd		1,27
time	1,7	1,7
tmpwatch	2.9,16	
traceroute	2.0.14	2.0.22
ttmkfdir	3.0.9	
tzdata	2023c	2023c
tzdata-java	2023c	
udev	173	

Package	AL1 AMI	AL2 AMI
unzip	6.0	6.0
update-motd	1.0.1	1.1.2
upstart	0,6,5	
usermode		1,111
ustr	1.0.4	1.0.4
util-linux	2,23,2	2,30,2
vim-common	9,0,1712	9,0,2081
vim-data	9,0,1712	9,0,2081
vim-enhanced	9,0,1712	9,0,2081
vim-filesystem	9,0,1712	9,0,2081
vim-minimal	9,0,1712	9,0,2081
virt-what		1,18
wget	1,18	1.14
which	2,19	2,20
words	3.0	3.0
xfsdump		3.1.8
xfsprogs		5.0.0
xorg-x11-font-utils	7.2	
xorg-x11-fonts-Type1	7.2	
xxd	9,0,1712	9,0,2081

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

Vergleich von Paketen, die auf Container-Images installiert sind AL1 und AL2 Basiscontainer-Images

Package	AL1 Container	AL2 Behälter
amazon-linux-extras		2.0.3
basesystem	10.0	10.0
bash	4.2.46	4.2,46
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023,2,62	2023,2,62

Package	AL1 Container	AL2 Behälter
chkconfig	1.3.49,3	1.7.4
coreutils	8,22	8,22
cpio		2.12
curl	7,61,1	8.3,0
cyrus-sasl-lib	2.1.23	2.1.26
db4	4.7,25	
db4-utils	4,7,25	
diffutils		3.3
elfutils-libelf	0,168	0,176
expat	2.1.0	2.1.0
file-libs	5,37	5,11
filesystem	2,4,30	3.2
findutils		4.5.11
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
glib2	2,36,3	2,56,1
glibc	2,17	2,26
glibc-common	2,17	2,26
glibc-langpack-en		2,26
glibc-minimal-langpack		2,26

Package	AL1 Container	AL2 Behälter
gmp	6.0.0	6.0.0
gnupg2	2.0.28	2.0.22
gpgme	1.4.3	1.3.2
grep	2,20	2,20
gzip	1.5	
info	5.1	5.1
keyutils-libs	1,5.8	1.5.8
krb5-libs	1.15.1	1.15.1
libacl	2,2,49	2,2,51
libassuan	2.0.3	2.1.0
libattr	2,4,46	2,4,46
libblkid		2,30,2
libcap	2,16	2,54
libcom_err	1,43,5	1,42,9
libcrypt		2,26
libcurl	7,61,1	8.3,0
libdb		5.3.21
libdb-utils		5.3.21
libffi	3.0,13	3.0,13
libgcc		7.3.1

Package	AL1 Container	AL2 Behälter
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgpg-error	1.11	1.12
libicu	50,2	
libidn2	2.3.0	2.3.0
libmetalink		0.1.3
libmount		2,30,2
libnghttp2	1,33,0	1,41,0
libpsl	0.6.2	
libselinux	2.1.10	2.5
libsepol	2.1.7	2.5
libssh2	1.4.2	1.4.3
libstdc++		7.3.1
libstdc++72	7.2.1	
libtasn1	2.3	4,10
libunistring	0.9.3	0.9.3
libuuid		2,30,2
libverto	0,2,5	0,2,5
libxml2	2.9.1	2.9.1
libxml2-python27	2.9.1	

Package	AL1 Container	AL2 Behälter
lua	5.1.4	5.1.4
make	3,82	
ncurses	5,7	6.0
ncurses-base	5,7	6.0
ncurses-libs	5,7	6.0
nspr	4,25,0	4,35,0
nss	3,53,1	3,90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3,53,1	3,90,0
nss-softokn-freebl	3,53,1	3,90,0
nss-sysinit	3,53,1	3,90,0
nss-tools	3,53,1	3,90,0
nss-util	3,53,1	3,90,0
OpenLDAP	2,4,40	2,4,44
OpenSSL	1,2k	
openssl-libs		1,2k
p11-kit	0,18,5	0,23,22
p11-kit-trust	0,18,5	0,23,22
pcre	8,21	8,32
pinentry	0,7.6	0.8.1

Package	AL1 Container	AL2 Behälter
pkgconfig	0,27,1	
popt	1.13	1.13
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0,5.3
python		2.7.18
python-iniparse		0.4
python-libs		2.7.18
python-pycurl		7.19.0
python-urlgrabber		3,10
python2-rpm		4.11.3
python27	2.7.18	
python27-chardet	2.0.1	
python27-iniparse	0.3.1	
python27-kitchen	1.1.1	
python27-libs	2.7.18	
python27-pycurl	7.19.0	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	
python27-pyxattr	0.5.0	

Package	AL1 Container	AL2 Behälter
python27-urlgrabber	3,10	
pyxattr		0.5.1
readline	6.2	6.2
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-python27	4.11.3	
sed	4.2.1	4.2.2
Einrichten	2.8.14	2,8,71
shared-mime-info	1.1	1.8
sqlite	3.7,17	3.7.17
sysctl-defaults	1,0	
system-release	2018,03	2
tar	1,26	
tzdata	2023c	2023c
vim-data		9.0.2081
vim-minimal		9,0,2081
xz-libs	5.2.2	5.2.2
yum	3.4.3	3.4.3
yum-metadata-parser	1.1.4	1.1.4

Package	AL1 Container	AL2 Behälter
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 auf Amazon EC2

> **Note**
>
> AL2 ist nicht mehr die aktuelle Version von Amazon Linux. AL2023 ist der Nachfolger von. AL2 Weitere Informationen finden Sie unter AL2 Comparing and AL2 023 und in der Liste der Paketänderungen in AL2 023 im AL2023-Benutzerhandbuch.

Themen

Starten Sie die EC2 Amazon-Instance mit AL2 AMI

Sie können eine EC2 Amazon-Instance mit dem AL2 AMI starten. Weitere Informationen finden Sie unter Schritt 1: Eine Instance starten.

Finden Sie das neueste AL2 AMI mit Systems Manager

Amazon EC2 stellt AWS Systems Manager öffentliche Parameter für public bereit AWS , die von AMIs verwaltet werden und die Sie beim Starten von Instances verwenden können. Beispielsweise

`/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-default-hvm-x86_64-gp2` ist der Parameter EC2 -provided in allen Regionen verfügbar und verweist immer auf die neueste Version des AL2 AMI in einer bestimmten Region.

Informationen zum aktuellen AL2 023-AMI finden Sie unter AWS Systems Manager Erste Schritte mit AL2 023.

Die öffentlichen Amazon EC2 AMI-Parameter sind über den folgenden Pfad verfügbar:

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

Sie können eine Liste aller Amazon Linux-Geräte AMIs in der aktuellen AWS Region anzeigen, indem Sie den folgenden AWS CLI Befehl ausführen.

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

So starten Sie eine Instance mit einem öffentlichen Parameter:

Im folgenden Beispiel wird der öffentliche Parameter EC2 -provided verwendet, um eine `m5.xlarge` Instance mit dem neuesten AL2 AMI zu starten.

Um den Parameter im Befehl anzugeben, verwenden Sie die folgende Syntax: `resolve:ssm:`*`public-parameter`*, wobei `resolve:ssm` das Standardpräfix und `public-parameter` der Pfad und Name des öffentlichen Parameters ist.

In diesem Beispiel sind die Parameter `--count` und `--security-group` nicht enthalten. Der Standardwert für `--count` lautet 1. Wenn Sie über eine Standard-VPC und eine Standardsicherheitsgruppe verfügen, werden diese verwendet.

```
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
```

Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Verwenden von öffentlichen Parametern.

Grundlegendes zu Amazon Linux 2-AMI-Namen

Amazon Linux 2-AMI-Namen verwenden das folgende Benennungsschema:

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

- Minimal AMIs enthält einen minimierten Satz vorinstallierter Pakete, um die Image-Größe zu reduzieren.
- Kernel-Version bestimmt die Kernel-Version, die auf dem jeweiligen AMI vorinstalliert ist:
  - `kernel-5.10`wählt die Linux-Kernel-Version 5.10 aus. Dies ist die empfohlene Kernel-Version für AL2.
  - `kernel-default`wählt den empfohlenen Standardkernel für aus AL2. Es ist ein Alias für Kernel-5.10.
  - `kernel-4.14`wählt die Linux-Kernel-Version 4.14 aus. Dies wird nur aus Gründen der Kompatibilität mit älteren AMI-Versionen bereitgestellt. Verwenden Sie diese Version nicht für den Start neuer Instances. Gehen Sie davon aus, dass dieses AMI nicht mehr unterstützt wird.
  - Ein spezieller Satz von AMI-Namen existiert ohne Verweis auf einen bestimmten Kernel. Dies AMIs sind Alias für Kernel-4.14. Diese AMIs werden nur aus Gründen der Kompatibilität mit älteren AMI-Versionen bereitgestellt. Verwenden Sie diesen AMI-Namen nicht für den Start neuer Instances. Erwarten Sie, dass der Kernel für diese AMIs aktualisiert wird.
- x86_64/aarch64 bestimmt die CPU-Plattform, auf der das AMI ausgeführt werden soll. Wählen Sie x86_64 für Intel- und AMD-basierte Instances aus. EC2 Wählen Sie aarch64 für Graviton-Instanzen aus. EC2
- ebs/gp2 bestimmt den EBS-Volumetyp, der zur Bereitstellung des jeweiligen AMI verwendet wird. Weitere Informationen finden Sie unter EBS-Volumetypen. Wählen Sie immer gp2 aus.

Stellen Sie eine Connect zu einer EC2 Amazon-Instance her

Es gibt mehrere Möglichkeiten, eine Verbindung zu Ihrer Amazon Linux-Instance herzustellen, darunter SSH und EC2 Instance Connect. AWS Systems Manager Session Manager Weitere Informationen finden Sie unter Connect to your Linux Instance im EC2 Amazon-Benutzerhandbuch.

SSH-Benutzer und sudo

Amazon Linux erlaubt standardmäßig keine Remote `root` Secure Shell (SSH). Außerdem ist die Passwortauthentifizierung deaktiviert, um Brute-Force-Angriffe zu verhindern. Sie können die Anmeldung bei einer Amazon Linux Instance über SSH aktivieren, indem Sie Ihr Schlüsselpaar

beim Start der Instance bereitstellen. Außerdem müssen Sie die Sicherheitsgruppe für den Start der Instance so konfigurieren, dass der Zugriff über SSH erlaubt ist. Standardmäßig ist das einzige Konto, das sich remote über SSH anmelden kann,. `ec2-user` Dieses Konto hat auch sudo Rechte. Wenn Sie die `root` Fernanmeldung aktivieren, beachten Sie, dass diese weniger sicher ist, als sich auf Schlüsselpaare und einen sekundären Benutzer zu verlassen.

AL2 AMI-Boot-Modus

AL2 AMIs haben keinen Startmodus-Parameter gesetzt. Instances, die von gestartet werden, AL2 AMIs folgen dem Standardwert für den Startmodus des Instance-Typs. Weitere Informationen finden Sie unter Startmodi im EC2 Amazon-Benutzerhandbuch.

Paket-Repository

Diese Information bezieht sich auf AL2. Informationen zu AL2 023 finden Sie unter Pakete und Betriebssystemupdates verwalten in AL2 023 im Amazon Linux 2023-Benutzerhandbuch.

AL2 und AL1 sind für die Verwendung mit Online-Paket-Repositorys konzipiert, die in jeder EC2 AWS Amazon-Region gehostet werden. Die Repositorys sind in allen Regionen verfügbar; der Zugriff erfolgt mithilfe des yum-Aktualisierungstools. Dadurch, dass die Repositorys in jeder Region gehostet werden, können wir Aktualisierungen schnell und ohne jegliche Datenübertragungskosten bereitstellen.

> **Important**
>
> Die letzte Version von AL1 hat am 31. Dezember 2023 das Ende der Laufzeit erreicht und wird ab dem 1. Januar 2024 keine Sicherheitsupdates oder Bugfixes mehr erhalten. Weitere Informationen finden Sie unter Amazon Linux AMI end-of-life.

Wenn Sie keine Daten oder Anpassungen für Ihre Instances beibehalten müssen, können Sie neue Instances mit dem aktuellen AL2 AMI starten. Wenn Sie Daten oder Anpassungen für Ihre Instances aufbewahren müssen, können Sie diese Instances über die Amazon Linux-Paket-Repositorys verwalten. Diese Repositorys enthalten alle aktualisierten Pakete. Sie können diese Aktualisierungen in Ihren ausgeführten Instances installieren. Frühere Versionen des AMI und der Aktualisierungspakete können weiterhin verwendet werden, auch wenn neue Versionen veröffentlicht werden.

> **Note**
>
> Informationen zum Aktualisieren und Installieren von Paketen ohne Internetzugang auf einer EC2 Amazon-Instance finden Sie unter Wie kann ich Yum aktualisieren oder Pakete ohne Internetzugang auf meinen EC2 Amazon-Instances installieren, auf denen AL1, AL2, oder AL2 023 ausgeführt wird?

Für die Installation von Paketen verwenden Sie den folgenden Befehl:

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

Wenn Sie feststellen, dass Amazon Linux die von Ihnen benötigte Anwendung nicht enthält, können Sie die Anwendung direkt auf Ihrer Amazon-Linux-Instance installieren. Amazon Linux verwendet RPMs und yum für die Paketverwaltung, und das ist wahrscheinlich der direkteste Weg, neue Anwendungen zu installieren. Überprüfen Sie zunächst, ob eine Anwendung in unserem zentralen Amazon-Linux-Repository verfügbar ist, da dort viele Anwendungen verfügbar sind. Von dort aus können Sie diese Anwendungen zu Ihrer Amazon Linux-Instance hinzufügen.

Um Ihre Anwendungen auf eine ausgeführte Amazon-Linux-Instance hochzuladen, verwenden Sie scp oder sftp und konfigurieren anschließend die Anwendung, indem Sie sich bei Ihrer Instance anmelden. Sie können Ihre Anwendungen außerdem mit der Aktion PACKAGE_SETUP aus dem enthaltenen cloud-init-Paket beim Starten der Instance hochladen. Weitere Informationen finden Sie unter Verwenden Sie Cloud-Init auf AL2.

Sicherheits-Updates

Sicherheitsupdates werden mithilfe der Paket-Repositorys bereitgestellt. Sowohl Sicherheitsupdates als auch aktualisierte AMI-Sicherheitswarnungen werden im Amazon Linux Security Center veröffentlicht. Weitere Informationen zu AWS -Sicherheitsrichtlinien oder zum Melden eines Sicherheitsproblems finden Sie unter AWS -Cloud-Sicherheit.

AL1 und AL2 sind so konfiguriert, dass sie kritische oder wichtige Sicherheitsupdates beim Start herunterladen und installieren. Kernel-Updates sind in dieser Konfiguration nicht enthalten.

Im AL2 Jahr 023 hat sich diese Konfiguration im Vergleich zu AL1 und AL2 geändert. Weitere Informationen zu Sicherheitsupdates für AL2 023 finden Sie unter Sicherheitsupdates und Funktionen im Amazon Linux 2023 User Guide.

Wir empfehlen Ihnen, nach dem Start die erforderlichen Aktualisierungen für Ihren Anwendungsfall vorzunehmen. Beispielsweise möchten Sie möglicherweise alle Updates (nicht nur Sicherheitsupdates) beim Start anwenden oder jedes Update auswerten und nur die Updates anwenden, die für Ihr System gelten. Dies wird mit Hilfe der folgenden cloud-init-Einstellung gesteuert: `repo_upgrade`. Der folgende Ausschnitt aus der cloud-init-Konfiguration zeigt, wie Sie die Einstellungen in dem Benutzerdaten-Text ändern können, den Sie an die Instance-Initialisierung übergeben:

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

Die möglichen Werte für `repo_upgrade` sind wie folgt:

`critical`

Anwenden ausstehender wichtiger Sicherheitsupdates.

`important`

Anwenden herausragend wichtiger und wichtiger Sicherheitsupdates.

`medium`

Anwenden herausragend wichtiger, wichtiger und mittlerer Sicherheitsupdates.

`low`

Anwenden aller ausstehenden Sicherheitsupdates an, einschließlich Sicherheitsupdates mit niedrigem Schweregrad.

`security`

Installieren ausstehender kritischer oder wichtiger Aktualisierungen, die Amazon als Sicherheitsupdates gekennzeichnet hat.

`bugfix`

Installieren von Aktualisierungen, die Amazon als Fehlerbehebungen gekennzeichnet hat. Fehlerbehebungen decken eine größere Anzahl von Aktualisierungen ab; dazu gehören Sicherheitsupdates und Patches für eine Reihe von anderen, kleineren Fehlern.

`all`

Installieren Sie alle verfügbaren Aktualisierungen, unabhängig davon, wie sie klassifiziert werden.

`none`

Installieren Sie keine Updates beim Startup der Instance.

> **Hinweis**
>
> Amazon Linux kennzeichnet keine Updates als`bugfix`. Um nicht sicherheitsrelevante Updates von Amazon Linux anzuwenden, verwenden Sie`repo_upgrade: all`.

Die Standardeinstellung für `repo_upgrade` ist „security”. Das heißt, wenn Sie in Ihren Benutzerdaten keinen anderen Wert angeben, führt Amazon Linux standardmäßig beim Starten die Sicherheitsupgrades für alle derzeit installierten Pakete aus. Amazon Linux benachrichtigt Sie außerdem über Aktualisierungen der installierten Pakete, indem bei der Anmeldung die Anzahl der verfügbaren Aktualisierungen über die `/etc/motd`-Datei aufgelistet wird. Sie installieren diese Aktualisierungen, indem Sie den Befehl sudo yum upgrade in der Instance ausführen.

Repository-Konfiguration

Für AL1 und AMIs sind eine Momentaufnahme der Pakete AL2, die zum Zeitpunkt der Erstellung des AMI verfügbar waren, mit Ausnahme von Sicherheitsupdates. Bei allen Paketen, die sich nicht auf dem ursprünglichen AMI befinden, sondern zur Laufzeit installiert wurden, handelt es sich um die neueste verfügbare Version. Führen Sie den Befehl aus AL2, um die neuesten verfügbaren Pakete für zu erhaltenyum update -y.

> **Tipp zur Problembehebung**
>
> Wenn bei der Ausführung yum update von Nano-Instance-Typen ein `cannot allocate memory` Fehler auftritt`t3.nano`, z. B. müssen Sie möglicherweise Swap-Speicherplatz zuweisen, um das Update zu aktivieren.

Für AL2 023 hat sich die Repository-Konfiguration im Vergleich zu AL1 und geändert. AL2 Weitere Informationen zum AL2 023-Repository finden Sie unter Pakete und Betriebssystemupdates verwalten.

Versionen bis AL2 023 wurden so konfiguriert, dass sie einen kontinuierlichen Fluss von Updates für die Übertragung von einer Nebenversion von Amazon Linux zur nächsten Version, auch Rolling

Releases genannt, bereitstellen. Als bewährte Methode empfehlen wir, Ihr AMI auf das neueste verfügbare AMI zu aktualisieren, anstatt alte zu starten AMIs und Updates anzuwenden.

Direkte Upgrades zwischen den wichtigsten Amazon Linux-Versionen, z. B. von bis AL2 oder von AL1 AL2 bis AL2 023, werden nicht unterstützt. Weitere Informationen finden Sie unter Amazon Linux-Verfügbarkeit.

Verwenden Sie Cloud-Init auf AL2

Das Cloud-Init-Paket ist eine von Canonical entwickelte Open-Source-Anwendung, die zum Bootstrap von Linux-Images in einer Cloud-Computing-Umgebung wie Amazon verwendet wird. EC2 Amazon Linux enthält eine angepasste Version von cloud-init. Auf diese Weise können Sie Aktionen angeben, die beim Booten auf Ihrer Instance ausgeführt werden sollen. Sie können die gewünschten Aktionen beim Start einer Instance über die Benutzerdatenfelder an cloud-init übergeben. Das bedeutet, dass Sie Common AMIs für viele Anwendungsfälle verwenden und sie beim Start dynamisch konfigurieren können. Amazon Linux verwendet cloud-init auch für die Anfangskonfiguration des ec2-user-Kontos.

Weitere Informationen finden Sie in der cloud-init-Dokumentation.

Amazon Linux verwendet die cloud-init-Aktionen aus `/etc/cloud/cloud.cfg.d` und `/etc/cloud/cloud.cfg`. Sie können Ihre eigenen cloud-init-Aktionsdateien unter erstelle `/etc/cloud/cloud.cfg.d`. Alle Dateien in diesem Verzeichnis werden von cloud-init eingelesen. Sie werden in lexikografischer Reihenfolge eingelesen, wobei später eingelesene Dateien die Werte in früher eingelesenen Dateien überschreiben.

Das cloud-init-Paket führt diese (und andere) allgemeine Konfigurationsaufgaben für Instances während des Bootvorgangs durch:

- Einstellen des Standard-Gebietsschemas.
- Einstellen des Hostnamens.
- Analysieren und Verarbeiten von Benutzerdaten.
- Generieren privater SSH-Schlüssel für den Host.
- Hinzufügen der öffentlichen SSH-Schlüssel eines Benutzers zu `.ssh/authorized_keys`, um eine einfache Anmeldung und Administration zu ermöglichen.
- Vorbereiten der --Repositorys für die Paketverwaltung.
- Verarbeiten der in den Benutzerdaten definierten Paketaktionen.

- Führen Sie Benutzerskripts aus, die in Benutzerdaten gefunden wurden.
- Mounten von Instance-Speicher-Volumes, falls zutreffend.
  - Standardmäßig wird das Instance-Speicher-Volume `ephemeral0` unter `/media/ephemeral0` gemountet – wenn es vorhanden ist und ein gültiges Dateisystem enthält; andernfalls wird es nicht gemountet.
  - Standardmäßig werden alle Swap-Volumes gemountet, die der Instance zugeordnet sind (gilt nur für die Instance-Typen `m1.small` und `c1.medium`).
  - Sie können den Standard-Einhängepunkt für ein Instance-Speicher-Volume mithilfe der folgenden cloud-init-Anweisung überschreiben:

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

    Weitere Informationen zum Steuern von Mountvorgängen finden Sie unter Mounts in der cloud-init-Dokumentation.
  - Instance-Speicher-Volumes mit TRIM-Unterstützung werden beim Start einer Instance nicht formatiert, d. h. Sie müssen Sie partitionieren und formatieren, bevor Sie sie mounten können. Weitere Informationen finden Sie unter TRIMUnterstützung für Instance Store Volume. Sie können das `disk_setup`-Modul verwenden, um Instance-Speicher-Volumes während des Bootvorgangs zu partitionieren und zu formatieren. Weitere Informationen finden Sie unter Disk Setup in der cloud-init-Dokumentation.

Unterstützte Benutzerdatenformate

Das Cloud-Init-Paket unterstützt die Verarbeitung von Benutzerdaten in einer Vielzahl von Formaten:

- Gzip
  - Wenn Benutzerdaten gzip-komprimiert sind, dekomprimiert Cloud-Init die Daten und verarbeitet sie entsprechend.
- MIME, mehrteilig
  - Wenn Sie eine mehrteilige MIME-Datei verwenden, können Sie mehrere Datentypen angeben. Sie könnten beispielsweise sowohl ein Benutzerdatenskript als auch einen Cloud-Konfigurationstyp angeben. Jeder Teil der mehrteiligen Datei kann von cloud-init entsprechend verarbeitet werden, wenn es sich um ein unterstütztes Format handelt.

- Base64-Decodierung
  - Wenn Benutzerdaten Base64-codiert sind, bestimmt cloud-init, ob es die dekodierten Daten als einen der unterstützten Typen verstehen kann. Wenn die decodierten Daten lesbar sind, werden die Daten von vollständig decodiert und weiter verarbeitet. Wenn sie nicht lesbar sind, werden die Base64-Daten unverändert zurückgegeben.
- Benutzerdatenskript
  - Beginnt mit `#!` oder `Content-Type: text/x-shellscript`
  - Das Skript wird beim ersten Systemstartzyklus von `/etc/init.d/cloud-init-user-scripts` ausgeführt. Dies geschieht relativ spät während des Bootvorgangs (nachdem die Aktionen für die Ausgangskonfiguration durchgeführt wurden).
- Include-Datei
  - Beginnt mit `#include` oder `Content-Type: text/x-include-url`
  - Dabei handelt es sich um eine Datei mit einzuschließenden Inhalten. Die Datei enthält eine Liste von, eine pro Zeile. URLs Jeder von ihnen URLs wird gelesen, und ihr Inhalt durchläuft dasselbe Regelwerk. Der aus der URL gelesene Inhalt kann gzip-komprimiert oder Klartext sein. MIME-multi-part
- Cloud-Konfigurationsdaten
  - Beginnt mit `#cloud-config` oder `Content-Type: text/cloud-config`
  - Bei diesem Inhalt handelt es sich um Cloud-Konfigurationsdaten.
- Upstart-Job (wird nicht unterstützt auf AL2)
  - Beginnt mit `#upstart-job` oder `Content-Type: text/upstart-job`
  - Dieser Inhalt wird in einer Datei in gespeichert`/etc/init`, und Upstart verwendet den Inhalt wie andere Upstart-Jobs.
- Cloud-Boothook
  - Beginnt mit `#cloud-boothook` oder `Content-Type: text/cloud-boothook`
  - Dabei handelt es sich um Boothook-Daten. Sie werden in einer Datei unter `/var/lib/cloud` gespeichert und unmittelbar danach ausgeführt.
  - Das ist der am frühesten verfügbare Hook. Es gibt keinen Mechanismus, der garantiert, dass dieser nur ein Mal ausgeführt wird. Der Boothook muss selbst dafür sorgen. Er wird mit der Instance-ID in der Umgebungsvariablen `INSTANCE_ID` bereitgestellt. Verwenden Sie diese Variable, um einen once-per-instance Satz von Boothook-Daten bereitzustellen.

Instanzen konfigurieren AL2

Nachdem Sie Ihre AL2 Instance erfolgreich gestartet und sich bei ihr angemeldet haben, können Sie Änderungen daran vornehmen. Ihnen stehen viele Wege zur Konfiguration einer Instance offen, um die Anforderungen einer bestimmten Anwendung zu erfüllen. Die folgenden Aufgaben sollen Ihnen bei den ersten Schritten helfen.

Inhalt

Gängige Konfigurationsszenarien

Die Basisversion von Amazon Linux umfasst viele Softwarepakete and Serviceprogramme, die für grundlegende Servervorgänge benötigt werden. Allerdings stehen noch viele weitere Softwarepakete in verschiedenen Software-Repositorys zur Verfügung und Sie können sogar noch mehr Pakete aus Quellcode selbst erstellen. Weitere Informationen zum Installieren und Erstellen von Software von diesen Standorten finden Sie unter Software auf Ihrer AL2 Instance verwalten.

Amazon-Linux-Instances sind mit einem `ec2-user` vorkonfiguriert, aber Sie möchten möglicherweise andere Benutzer hinzufügen, die nicht über Super-User-Privilegien verfügen. Weitere Informationen zum Hinzufügen und Entfernen von Benutzern finden Sie unter Benutzer auf Ihrer Linux Instance verwalten im EC2 Amazon-Benutzerhandbuch.

Falls Sie über ein Netzwerk mit einem Domain-Namen verfügen, können Sie den Hostnamen einer Instance so verändern, dass sie sich als Teil dieser Domain identifiziert. Außerdem können Sie die Systemanzeige einen aussagekräftigeren Namen anzeigen lassen, ohne die Einstellungen des Hostnamens zu verändern. Weitere Informationen finden Sie unter Ändern Sie den Hostnamen Ihrer Instanz AL2 . Sie können eine Instance für die Verwendung eines Serviceanbieters für ein dynamisches DNS konfigurieren. Weitere Informationen finden Sie unter Richten Sie dynamisches DNS auf Ihrer Instance ein AL2 .

Wenn Sie eine Instance in Amazon starten EC2, haben Sie die Möglichkeit, Benutzerdaten an die Instance zu übergeben, die verwendet werden können, um allgemeine Konfigurationsaufgaben durchzuführen und sogar Skripts auszuführen, nachdem die Instance gestartet wurde. Sie können zwei Arten von Benutzerdaten an Amazon übergeben EC2: Cloud-Init-Direktiven und Shell-Skripte. Weitere Informationen finden Sie unter Befehle auf Ihrer Linux Instance beim Start ausführen im EC2 Amazon-Benutzerhandbuch.

Software auf Ihrer AL2 Instance verwalten

Die Basisversion von Amazon Linux umfasst viele Softwarepakete and Serviceprogramme, die für grundlegende Servervorgänge benötigt werden.

Diese Information bezieht sich auf AL2. Informationen zu AL2 023 finden Sie unter Pakete und Betriebssystemupdates verwalten in AL2 023 im Amazon Linux 2023-Benutzerhandbuch.

Software sollte nach Möglichkeit auf dem neuesten Stand gehalten werden. Viele Pakete einer Linux-Bereitstellung werden häufig aktualisiert, um Fehler zu beheben, Features hinzuzufügen und Sicherheitslücken zu schließen. Weitere Informationen finden Sie unter Aktualisieren Sie die Instanzsoftware auf Ihrer AL2 Instanz.

Standardmäßig werden AL2 Instances mit den folgenden aktivierten Repositorys gestartet:

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

In diesen Repositorys sind zwar viele Pakete verfügbar, von denen sie aktualisiert werden AWS, aber vielleicht gibt es ein Paket, das Sie installieren möchten und das in einem anderen Repository enthalten ist. Weitere Informationen finden Sie unter Fügen Sie Repositorys auf einer Instance AL2 hinzu. Weitere Informationen dazu, wie Sie Pakete in aktivierten Repositorys finden und installieren finden Sie unter Suchen und installieren Sie Softwarepakete auf einer AL2 Instanz.

Nicht alle Software steht als Paket in einem Repository zur Verfügung: Einige Software muss auf einer Instance aus ihrem Quellcode kompiliert werden. Weitere Informationen finden Sie unter Bereiten Sie die Kompilierung der Software auf einer AL2 Instanz vor.

AL2 Instanzen verwalten ihre Software mithilfe des Yum-Paketmanagers. Der Paketmanager „yum“ kann Software installieren, entfernen und aktualisieren sowie alle Abhängigkeiten eines Pakets verwalten.

Inhalt

Aktualisieren Sie die Instanzsoftware auf Ihrer AL2 Instanz

Software sollte nach Möglichkeit auf dem neuesten Stand gehalten werden. Pakete einer Linux-Bereitstellung werden häufig aktualisiert, um Fehler zu beheben, Features hinzuzufügen und Sicherheitslücken zu schließen. Wenn Sie eine Amazon Linux-Instance zum ersten Mal starten und eine Verbindung zu ihr herstellen, wird u. U. eine Meldung angezeigt, die Sie dazu auffordert, aus Sicherheitsgründen Softwarepakete zu aktualisieren. In diesem Abschnitt wird beschrieben, wie Sie das gesamte System oder nur ein einzelnes Paket aktualisieren.

Diese Information bezieht sich auf AL2. Informationen zu AL2 023 finden Sie unter Pakete und Betriebssystemupdates verwalten in AL2 023 im Amazon Linux 2023-Benutzerhandbuch.

Informationen zu Änderungen und Aktualisierungen von finden Sie in den AL2 AL2 Versionshinweisen.

Informationen zu Änderungen und Aktualisierungen von Version AL2 023 finden Sie in den Versionshinweisen zu AL2 023.

> **Important**
>
> Wenn Sie eine EC2 Instance gestartet haben, die ein Amazon Linux 2-AMI in einem IPv6 Nur-Only-Subnetz verwendet, müssen Sie eine Verbindung mit der Instance herstellen und sie ausführen. `sudo amazon-linux-https disable` Dadurch kann Ihre AL2 Instance über den HTTP-Patch-Service eine Verbindung zum yum Repository in S3 IPv6 herstellen.

Um alle Pakete auf einer AL2 Instanz zu aktualisieren

1. (Optional) Starten Sie eine screen-Sitzung im Shell-Fenster. Manchmal treten u. U. Netzwerkunterbrechungen auf, die die SSH-Verbindung zur Instance unterbrechen. Wenn dies während einer lang andauernden Softwareaktualisierung geschieht, verwirrt dies die Instance,

sie kann aber wiederhergestellt werden. Eine screen-Sitzung ermöglicht Ihnen, die Aktualisierung auch im Falle einer Verbindungsunterbrechung fortzusetzen, und später können Sie problemlos eine neue Verbindung zur Sitzung herstellen.

a. Führen Sie den Befehl screen aus, um die Sitzung zu beginnen.

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

b. Wird die Verbindung der Sitzung getrennt, melden Sie sich erneut auf der Instance an und rufen Sie die Liste der verfügbaren Bildschirme auf.

```
[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. Stellen Sie mithilfe des Befehls screen -r und der Prozess-ID des vorherigen Befehls erneut eine Verbindung zu dem Bildschirm her.

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

d. Wenn Sie screen nicht weiter benötigen, verwenden Sie den Befehl exit, um die Sitzung zu schließen.

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

2. Führen Sie den Befehl yum update aus. Fügen Sie optional das Flag `--security` hinzu, um nur Sicherheitsaktualisierungen zu installieren.

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

3. Überprüfen Sie die aufgeführten Pakete, geben Sie **y** ein und drücken Sie die Eingabetaste, um die Aktualisierungen anzunehmen. Die Aktualisierung aller Pakete eines Systems nimmt u. U. mehrere Minuten in Anspruch. Die Ausgabe von yum zeigt den Status der Aktualisierung an, während diese durchgeführt wird.
4. (Optional) Starten Sie Ihre Instance neu, um sicherzustellen, dass Sie die neuesten Pakete und Bibliotheken aus Ihrem Update verwenden. Kernel-Updates werden erst geladen, wenn ein Neustart erfolgt. Auf Aktualisierungen der `glibc`-Bibliotheken sollte ebenso ein Neustart folgen. Für Aktualisierungen der Pakete, die Services steuern, reicht u. U. der Neustart des

Service aus, um Aktualisierungen zu aktivieren, aber ein Systemneustart stellt sicher, dass alle durchgeführten Paket- und Bibliothekaktualisierungen vollständig geladen werden.

Um ein einzelnes Paket auf einer AL2 Instance zu aktualisieren

Wenden Sie die folgende Vorgehensweise an, um anstatt des ganzen Systems nur ein einzelnes Paket (und seine Abhängigkeiten) zu aktualisieren.

1. Führen Sie den Befehl yum update mit dem Namen des Pakets aus, das Sie aktualisieren möchten.

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

2. Überprüfen Sie die aufgeführten Paketinformationen, geben Sie **y** ein und drücken Sie die Eingabetaste, um die Aktualisierung(en) anzunehmen. Manchmal wird mehr als ein Paket aufgeführt, falls Probleme mit Paketabhängigkeiten bestehen. Die Ausgabe von yum zeigt den Status der Aktualisierung an, während diese durchgeführt wird.
3. (Optional) Starten Sie Ihre Instance neu, um sicherzustellen, dass Sie die neuesten Pakete und Bibliotheken aus Ihrem Update verwenden. Kernel-Updates werden erst geladen, wenn ein Neustart erfolgt. Auf Aktualisierungen der `glibc`-Bibliotheken sollte ebenso ein Neustart folgen. Für Aktualisierungen der Pakete, die Services steuern, reicht u. U. der Neustart des Service aus, um Aktualisierungen zu aktivieren, aber ein Systemneustart stellt sicher, dass alle durchgeführten Paket- und Bibliothekaktualisierungen vollständig geladen werden.

Fügen Sie Repositorys auf einer Instance AL2 hinzu

Diese Information bezieht sich auf. AL2 Informationen zu AL2 023 finden Sie unter Deterministische Upgrades durch versionierte Repositorys auf AL2 023 im Amazon Linux 2023 User Guide.

Standardmäßig werden AL2 Instances mit den folgenden aktivierten Repositorys gestartet:

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

In diesen Repositorys befinden sich viele Pakete, die von Amazon Web Services aktualisiert werden, aber möglicherweise möchten Sie ein Paket installieren, das in einem anderen Repository enthalten ist.

Zum Installieren eines Pakets aus einem anderen Repository mithilfe von yum müssen Sie die Daten des Repository der Datei `/etc/yum.conf` oder seiner eigenen *`repository`*`.repo`-Datei im Verzeichnis `/etc/yum.repos.d` hinzufügen. Dies kann manuell erfolgen, aber die meisten yum-Repositorys verfügen über eigene *`repository`*`.repo`-Dateien an ihrer Repository-URL.

Stellen Sie wie folgt fest, welche yum-Repositorys bereits installiert sind:

Mit dem folgenden Befehl führen Sie die installierten yum-Repositorys auf:

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

Die resultierende Ausgabe führt alle installierten Repositorys und ihre jeweiligen Status auf. Aktivierte Repositorys zeigen die Anzahl der Pakete an, die sie enthalten.

Fügen Sie ein yum-Repository wie folgt zur Datei hinzu /etc/yum.repos.d

1. Suchen Sie den Speicherort der Datei `.repo`. Dieser hängt von dem Repository ab, das Sie hinzufügen. In diesem Beispiel befindet sich die Datei `.repo` unter `https://www.`*`example`*`.com/`*`repository`*`.repo`.
2. Erstellen Sie ein Repository mit dem Befehl 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
   ```

Nach der Installation von Repositorys müssen diese wie folgt aktiviert werden.

Aktivieren Sie ein yum-Repository in wie folgt /etc/yum.repos.d

Verwenden Sie den Befehl yum-config-manager mit dem `--enable` *`repository`*-Namespace. Der folgende Befehl aktiviert das Repository „Extra Packages for Enterprise Linux (EPEL)“ des Projekts „Fedora“. Standardmäßig steht dieses Repository auf `/etc/yum.repos.d`-Instances unter Amazon Linux AMI zur Verfügung, ist aber nicht aktiviert.

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

Weitere Informationen und den Download der neuesten Version dieses Pakets finden Sie unter https://fedoraproject. org/wiki/EPEL.

Suchen und installieren Sie Softwarepakete auf einer AL2 Instanz

Sie können ein Paketverwaltungstool verwenden, um Softwarepakete zu suchen und zu installieren. In Amazon Linux 2 ist das Standard-Tool zur Verwaltung von SoftwarepaketenYUM. In AL2 023 ist DNF das Standard-Tool zur Verwaltung von Softwarepaketen. Weitere Informationen finden Sie unter Package Management Tool im Amazon Linux 2023 User Guide.

Suchen Sie nach Softwarepaketen auf einer AL2 Instance

Verwenden Sie den Befehl yum search, um nach den Beschreibungen der Pakete zu suchen, die in den konfigurierten Repositorys zur Verfügung stehen. Diese Funktion ist besonders hilfreich, wenn Sie den genauen Namen des zu installierenden Pakets nicht kennen. Hängen Sie die Stichwortsuche einfach an den Befehl an. Grenzen Sie die Suchanfragen mit Anführungszeichen ab, wenn Sie mehrere Stichwortsuchen anhängen.

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

Es folgt eine Beispielausgabe.

```
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
```

Mehrere Schlüsselwortsuchanfragen in Anführungszeichen geben nur Ergebnisse zurück, die exakt zu der Anfrage passen. Falls Sie das gesuchte Paket nicht finden, suchen Sie nur nach einem Stichwort und überfliegen Sie die Ergebnisse. Sie können auch Synonyme der Stichwörter verwenden, um die Suche zu verallgemeinern.

Weitere Informationen zu Paketen für AL2 finden Sie unter:

- AL2 Extras-Bibliothek
- Paket-Repository

Installieren Sie Softwarepakete auf einer AL2 Instanz

In AL2 durchsucht das Yum-Paketverwaltungstool alle Ihre aktivierten Repositorys nach verschiedenen Softwarepaketen und behandelt alle Abhängigkeiten im Softwareinstallationsprozess. Informationen zur Installation von Softwarepaketen in AL2 023 finden Sie unter Verwalten von Paketen und Betriebssystemupdates im Amazon Linux 2023-Benutzerhandbuch.

So installieren Sie ein Paket aus einem Repository:

Verwenden Sie den yum install ***package*** Befehl und *package* ersetzen Sie ihn durch den Namen der zu installierenden Software. Geben Sie beispielsweise den folgenden Befehl ein, um den links textbasierten Webbrowser Links zu installieren:

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

So installieren Sie RPM-Paketdateien, die Sie heruntergeladen haben:

Sie können auch den Befehl yum install verwenden, um RPM-Paketdateien zu installieren, die Sie aus dem Internet heruntergeladen haben. Hängen Sie dazu anstatt des Namens eines Repository-Pakets den Pfad der RPM-Datei an den Installationsbefehl an.

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

So erstellen Sie eine Liste der installierten Pakete:

Verwenden Sie den folgenden Befehl, um eine Liste der installierten Pakete auf Ihrer Instance anzuzeigen.

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

Bereiten Sie die Kompilierung der Software auf einer AL2 Instanz vor

Open-Source-Software ist im Internet verfügbar, ohne dass sie vorkompiliert und in einem Paketarchiv zum Download bereitgestellt wurde. Irgendwann stoßen Sie wahrscheinlich auf ein Softwarepaket, dass Sie selbst aus seinem Quellcode kompilieren möchten. Damit Ihr System Software in AL2 und Amazon Linux kompilieren kann, müssen Sie mehrere Entwicklungstools installieren, z. B. makegcc, undautoconf.

Da die Softwarekompilierung keine Aufgabe ist, die jede EC2 Amazon-Instance benötigt, werden diese Tools nicht standardmäßig installiert, sondern sie sind in einer Paketgruppe namens „Development Tools“ verfügbar, die einfach mit dem yum groupinstall Befehl zu einer Instance hinzugefügt werden kann.

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

Software-Quellcodepakete stehen häufig (von Websites wie https://github.com/und http://sourceforge.net/) als komprimierte Archivdatei, die als Tarball bezeichnet wird, zum Herunterladen zur Verfügung. Sie verfügen üblicherweise über die Dateierweiterung `.tar.gz`. Diese Archive lassen sich mithilfe des Befehls tar dekomprimieren.

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

Wenn Sie das Quellcodepaket dekomprimiert und extrahiert haben, suchen Sie die Datei `README` oder `INSTALL` im Quellcodeverzeichnis. Diese Dateien enthalten weitere Anleitungen zum Kompilieren und Installieren des Quellcodes.

So rufen Sie den Quellcode für Amazon Linux-Pakete ab

Amazon Web Services stellt den Quellcode von installierten Paketen zur Verfügung. Nutzen Sie zum Herunterladen des Quellcodes von installierten Paketen den Befehl yumdownloader --source.

Führen Sie den yumdownloader --source ***package*** Befehl aus, um den Quellcode für *package* herunterzuladen. Geben Sie beispielsweise den folgenden Befehl ein, um den Quellcode des Pakets `htop` zu installieren:

```
[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
```

Der Speicherort des Quell-RPM befindet sich in dem Verzeichnis, aus dem Sie den Befehl ausgeführt haben.

Kontrolle des Prozessorstatus für Ihre EC2 AL2 Amazon-Instance

C-Status steuern die Ruhezustände, in die ein Kern eintreten kann, wenn er sich im Leerlauf befindet. C-Zustände sind von C0 (Arbeitszustand, in dem der Core „wach“ ist und Anweisungen ausführt) bis C6 („tiefster“ Leerlaufzustand, in dem ein Core ausgeschaltet ist) nummeriert.

P-Status steuern die gewünschte Leistung (in CPU-Frequenz) eines Kerns. P-Zustände sind ab P0 (höchste Performancestufe, in der Intel Turbo Boost-Technologie für den Core eingesetzt werden kann, um ggf. die Frequenz zu erhöhen) über P1 (in diesem P-Zustand wird die maximale Basisfrequenz angefordert) bis P15 (geringstmögliche Frequenz) nummeriert.

Es kann ratsam sein, die Einstellungen für den C- bzw. P-Zustand zu ändern, um die Konsistenz der Prozessorleistung zu erhöhen, die Latenz zu reduzieren oder Ihre Instance für einen bestimmten Workload zu optimieren. Die Standardeinstellungen für den C- und P-Zustand sind auf maximale Performance ausgelegt. Dies ist für die meisten Workloads optimal. Erwägen Sie jedoch, mit den für diese Instances verfügbaren Einstellungen für den C- oder P-Zustand zu experimentieren, wenn Ihre Anwendung von einer verringerten Latenz auf Kosten von höheren Single- oder Dual-Core-Frequenzen oder von einer konsistenten Performance bei niedrigeren Frequenzen (im Gegensatz zu diskontinuierlichen Turbo Boost-Frequenzen) profitieren würde.

Informationen zu EC2 Amazon-Instance-Typen, mit denen das Betriebssystem C-Status und P-Status von Prozessoren steuern kann, finden Sie unter Prozessor-State-Steuerung für Ihre EC2 Amazon-Instance im EC2 Amazon-Benutzerhandbuch.

In den folgenden Abschnitten werden die unterschiedlichen Prozessorstatuskonfigurationen und die Überwachung der Auswirkungen Ihrer Konfiguration beschrieben. Diese Verfahren wurden für Amazon Linux geschrieben und gelten für Amazon Linux. Sie könnten jedoch auch für andere Linux-Distributionen mit einer Linux-Kernel-Version 3.9 oder neuer funktionieren.

> **Note**
>
> Bei den Beispielen auf dieser Seite wurde Folgendes verwendet:
>
> - Das turbostat-Dienstprogramm zeigt Informationen zur Prozessorfrequenz und zum C-Zustand an. Das turbostat-Dienstprogramm ist standardmäßig unter Amazon Linux verfügbar.
> - Der stress-Befehl simuliert eine Workload. Um stress zu installieren, aktivieren Sie zuerst das EPEL-Repository, indem Siesudo amazon-linux-extras install epel und dann sudo yum install -y stress ausführen.
>
> Wenn die Ausgabe die Informationen zum C-Zustand nicht anzeigt, schließen Sie die Option --debug im Befehl (sudo turbostat --debug stress ***<options>***) ein.

Inhalt

Höchste Performance mit maximaler Turbo Boost-Frequenz

Dies ist die Standardkonfiguration zum Steuern des Prozessorzustands für das Amazon Linux AMI und wird für die meisten Workloads empfohlen. Diese Konfiguration bietet die höchste Performance mit geringerer Variabilität. Wenn für inaktive Cores „tiefere“ Ruhezustände zugelassen werden, ist der thermische Spielraum vorhanden, der erforderlich ist, damit Single- oder Dual-Core-Prozesse ihr maximales Turbo Boost-Potenzial erreichen können.

Das folgende Beispiel enthält eine Instance vom Typ `c4.8xlarge` mit zwei aktiven Cores, die ihre maximale Turbo Boost-Prozessorfrequenz erreichen.

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

In diesem Beispiel laufen v CPUs 21 und 28 mit ihrer maximalen Turbo-Boost-Frequenz, weil die anderen Kerne in den C6 Ruhezustand übergegangen sind, um Strom zu sparen und sowohl Strom als auch thermischen Spielraum für die arbeitenden Kerne bereitzustellen. v CPUs 3 und 10 (jeweils teilen sich einen Prozessorkern mit v CPUs 21 und 28) befinden sich in dem C1 Zustand und warten auf Anweisungen.

Im folgenden Beispiel verrichten alle 18 Kerne aktiv Arbeit, sodass kein Spielraum für maximalen Turbo-Boost besteht, aber sie laufen alle mit der „All-Core-Turbo-Boost-Geschwindigkeit“ von 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   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
...
```

Hohe Performance und geringe Latenz durch die Beschränkung von tieferen C-Zuständen

Mit dem C-Zustand werden die Ruhezustandsebenen gesteuert, in denen sich ein Core im inaktiven Zustand befinden kann. Es kann ratsam sein, die C-Zustände zu steuern, um Ihr System im Hinblick auf Latenz und Performance zu optimieren. Das Versetzen von Cores in den Ruhezustand benötigt Zeit. Und auch wenn ein Core im Ruhezustand mehr Spielraum zur Nutzung einer höheren Frequenz durch einen anderen Core zulässt, dauert es auch wieder eine gewisse Zeit, bis der Core aus dem Ruhezustand erwacht und Arbeitsschritte ausführen kann. Falls sich beispielsweise ein Core, der für die Verarbeitung von Netzwerkpaketunterbrechungen zugewiesen ist, im Ruhezustand befindet, kann es bei der Verarbeitung der Unterbrechung zu einer Verzögerung kommen. Sie können das System so konfigurieren, dass keine tieferen C-Zustände verwendet werden. Hierdurch wird die Latenz in Bezug auf die Prozessorreaktion reduziert, aber gleichzeitig wird auch der Turbo Boost-Spielraum für andere Cores verringert.

Ein häufiges Szenario zum Deaktivieren von tieferen Ruhezuständen ist die Nutzung einer Redis-Datenbankanwendung, bei der die Datenbank im Systemspeicher gespeichert wird, um für Abfragen eine möglichst geringe Reaktionszeit zu erzielen.

Um tiefere Schlafzustände zu begrenzen, aktivieren Sie AL2

1. Öffnen Sie die Datei `/etc/default/grub` mit einem Editor Ihrer Wahl.

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

2. Bearbeiten Sie die Zeile `GRUB_CMDLINE_LINUX_DEFAULT` und fügen Sie die Optionen `intel_idle.max_cstate=1` und `processor.max_cstate=1` hinzu, um `C1` als tiefstmöglichen C-Zustand für Cores im Leerlauf festzulegen.

```
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
```

   Die`intel_idle.max_cstate=1`-Option konfiguriert das C-Zustandslimit für Intel-basierte Instances, die `processor.max_cstate=1`-Option konfiguriert das C-Zustandslimit für AMD-basierte Instances. Sie können beide Optionen zu Ihrer Konfiguration hinzufügen. So können Sie mit einer einzigen Konfiguration das gewünschte Verhalten sowohl für Intel als auch AMD festlegen.

3. Speichern Sie die Datei und beenden Sie den Editor.
4. Führen Sie den folgenden Befehl aus, um die Bootkonfiguration erneut zu erstellen:

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

5. Starten Sie Ihre Instance neu, um die neue Kerneloption zu aktivieren.

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

So begrenzen Sie tiefere Ruhezustände für Amazon Linux AMI

1. Öffnen Sie die Datei `/boot/grub/grub.conf` mit einem Editor Ihrer Wahl.

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

2. Bearbeiten Sie die Zeile `kernel` des ersten Eintrags und fügen Sie die Optionen `intel_idle.max_cstate=1` und `processor.max_cstate=1` hinzu, um `C1` als tiefstmöglichen C-Zustand für Cores im Leerlauf festzulegen.

```
# 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
```

Die`intel_idle.max_cstate=1`-Option konfiguriert das C-Zustandslimit für Intel-basierte Instances, die `processor.max_cstate=1`-Option konfiguriert das C-Zustandslimit für AMD-basierte Instances. Sie können beide Optionen zu Ihrer Konfiguration hinzufügen. So können Sie mit einer einzigen Konfiguration das gewünschte Verhalten sowohl für Intel als auch AMD festlegen.

3. Speichern Sie die Datei und beenden Sie den Editor.
4. Starten Sie Ihre Instance neu, um die neue Kerneloption zu aktivieren.

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

Das folgende Beispiel enthält eine Instance vom Typ `c4.8xlarge` mit zwei aktiven Cores, für die die Core-Frequenz vom Typ „Turbo Boost für alle Cores“ genutzt wird.

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

```
...
```

In diesem Beispiel laufen die Kerne für Version CPUs 19 und 28 mit 3.2 GHz, und die anderen Kerne befinden sich im `C1` C-Status und warten auf Befehle. Für die aktiven Cores wird zwar nicht die maximale Turbo Boost-Frequenz erreicht, aber die inaktiven Cores können viel schneller auf neue Anforderungen reagieren, als dies im tieferen C-Zustand `C6` der Fall wäre.

Basis-Performance mit geringster Variabilität

Sie können die Variabilität der Prozessorfrequenz mit P-Zuständen reduzieren. Mit P-Zuständen wird die gewünschte Performance für einen Core gesteuert (nach CPU-Frequenz). Für die meisten Workloads wird im Zustand P0, in dem Turbo Boost angefordert wird, eine bessere Performance erzielt. Es kann aber sein, dass Sie für Ihr System eine konsistente Performance konfigurieren möchten, weil es bei der Aktivierung von Turbo Boost-Frequenzen zu einer diskontinuierlichen Performance kommen kann.

Intel Advanced Vector Extensions (AVX oder AVX2) -Workloads können bei niedrigeren Frequenzen eine gute Leistung erbringen, und AVX-Befehle können mehr Strom verbrauchen. Wenn der Prozessor bei einer niedrigeren Frequenz ausgeführt wird, indem Turbo Boost deaktiviert wird, kann die genutzte Leistungsmenge reduziert und die Geschwindigkeit konsistenter gehalten werden. Weitere Informationen zur Optimierung Ihrer Instance-Konfiguration und des Workload für AVX erhalten Sie auf der Intel-Website.

CPU-Leerlauf-Treiber steuern den P-Zustand. Neuere CPU-Generationen erfordern aktualisierte CPU-Leerlauf-Treiber, die der Kernelebene wie folgt entsprechen:

- Linux-Kernel-Versionen 6.1 und höher — Unterstützt Intel Granite Rapids (z. B. R8i)
- Linux-Kernel-Versionen 5.10 und höher — Unterstützt AMD Milan (zum Beispiel M6a)
- Linux-Kernel-Versionen 5.6 und höher — Unterstützt Intel Icelake (zum Beispiel M6i)

Führen Sie den folgenden Befehl aus, um festzustellen, ob der Kernel eines laufenden Systems die CPU erkennt.

```
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
```

Wenn die Ausgabe dieses Befehls auf fehlende Unterstützung hinweist, empfehlen wir Ihnen, den Kernel upzugraden.

In diesem Abschnitt wird beschrieben, wie Sie tiefere Ruhezustände begrenzen und Turbo Boost deaktivieren (durch Anforderung des P-Zustands P1), um für diese Arten von Workloads ein geringe Latenz und die geringstmögliche Variabilität der Prozessorgeschwindigkeit bereitzustellen.

Um tiefere Schlafzustände zu begrenzen und Turbo Boost einzuschalten AL2

1. Öffnen Sie die Datei `/etc/default/grub` mit einem Editor Ihrer Wahl.

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

2. Bearbeiten Sie die Zeile `GRUB_CMDLINE_LINUX_DEFAULT` und fügen Sie die Optionen `intel_idle.max_cstate=1` und `processor.max_cstate=1` hinzu, um `C1` als tiefstmöglichen C-Zustand für Cores im Leerlauf festzulegen.

   ```
   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
   ```

   Die`intel_idle.max_cstate=1`-Option konfiguriert das C-Zustandslimit für Intel-basierte Instances, die `processor.max_cstate=1`-Option konfiguriert das C-Zustandslimit für AMD-basierte Instances. Sie können beide Optionen zu Ihrer Konfiguration hinzufügen. So können Sie mit einer einzigen Konfiguration das gewünschte Verhalten sowohl für Intel als auch AMD festlegen.

3. Speichern Sie die Datei und beenden Sie den Editor.
4. Führen Sie den folgenden Befehl aus, um die Bootkonfiguration erneut zu erstellen:

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

5. Starten Sie Ihre Instance neu, um die neue Kerneloption zu aktivieren.

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

6. Führen Sie den folgenden Befehl aus, um Turbo Boost zu deaktivieren, wenn Sie die geringe Variabilität der Prozessorgeschwindigkeit benötigen, die im P-Zustand `P1` bereitgestellt wird.

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

7. Wenn die Verarbeitung Ihrer Workload abgeschlossen ist, können Sie Turbo Boost mit dem unten angegebenen Befehl wieder aktivieren.

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

So begrenzen Sie tiefere Ruhezustände und deaktivieren Turbo Boost für Amazon Linux AMI

1. Öffnen Sie die Datei `/boot/grub/grub.conf` mit einem Editor Ihrer Wahl.

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

2. Bearbeiten Sie die Zeile `kernel` des ersten Eintrags und fügen Sie die Optionen `intel_idle.max_cstate=1` und `processor.max_cstate=1` hinzu, um `C1` als tiefstmöglichen C-Zustand für Cores im Leerlauf festzulegen.

```
# 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
```

   Die`intel_idle.max_cstate=1`-Option konfiguriert das C-Zustandslimit für Intel-basierte Instances, die `processor.max_cstate=1`-Option konfiguriert das C-Zustandslimit für AMD-basierte Instances. Sie können beide Optionen zu Ihrer Konfiguration hinzufügen. So können Sie mit einer einzigen Konfiguration das gewünschte Verhalten sowohl für Intel als auch AMD festlegen.

3. Speichern Sie die Datei und beenden Sie den Editor.
4. Starten Sie Ihre Instance neu, um die neue Kerneloption zu aktivieren.

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

5. Führen Sie den folgenden Befehl aus, um Turbo Boost zu deaktivieren, wenn Sie die geringe Variabilität der Prozessorgeschwindigkeit benötigen, die im P-Zustand `P1` bereitgestellt wird.

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

6. Wenn die Verarbeitung Ihrer Workload abgeschlossen ist, können Sie Turbo Boost mit dem unten angegebenen Befehl wieder aktivieren.

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

Das folgende Beispiel zeigt eine `c4.8xlarge` Instanz mit zwei V, die CPUs aktiv mit der Basiskernfrequenz arbeiten, ohne Turbo Boost.

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

Die Kerne für v CPUs 21 und 28 arbeiten aktiv mit der Basisprozessorgeschwindigkeit von 2,9 GHz, und alle inaktiven Kerne laufen ebenfalls mit der Basisgeschwindigkeit im `C1` C-Zustand und sind bereit, Befehle anzunehmen.

I/O-Scheduler für AL2

Die I/O scheduler is a part of the Linux operating system that sorts and merges I/O Anfragen und bestimmt die Reihenfolge, in der sie verarbeitet werden.

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/OScheduler haben bei Solid-State-Geräten und virtualisierten Umgebungen weniger Wirkung. Dies liegt daran, dass sich der sequentielle und zufällige Zugriff bei Solid-State-Geräten nicht unterscheiden und der Host für virtualisierte Umgebungen eine eigene Planungsebene bereitstellt.

In diesem Thema wird der Amazon I/O Linux-Scheduler behandelt. Weitere Informationen über den I/O-Scheduler, der von anderen Linux-Verteilungen verwendet wird, finden Sie in der jeweiligen Dokumentation.

Themen

Unterstützte Scheduler

Amazon Linux unterstützt die folgenden I/O Scheduler:

- `deadline`— Der Deadline I/O Scheduler sortiert I/O Anfragen und bearbeitet sie in der effizientesten Reihenfolge. Es garantiert eine Startzeit für alle I/O request. It also gives I/O Anfragen, die zu lange ausstehen und eine höhere Priorität haben.
- `cfq`— Der Completely Fair Queueing (CFQ) I/O -Scheduler versucht, I/O resources between processes. It sorts and inserts I/O Anfragen fair den Warteschlangen pro Prozess zuzuordnen.
- `noop`— Die I/O scheduler inserts all I/O Noop-Anfragen (No Operation) werden einer FIFO-Warteschlange zugeordnet und dann zu einer einzigen Anfrage zusammengeführt. Dieser Scheduler führt keine Anforderungssortierung durch.

Standard-Scheduler

No Operation (noop) ist der I/O Standard-Scheduler für Amazon Linux. Dieser Scheduler wird aus folgenden Gründen verwendet:

- Viele Instance-Typen verwenden virtualisierte Geräte, bei denen der zugrunde liegende Host die Planung für die Instance durchführt.
- Solid-State-Geräte werden in vielen Instance-Typen verwendet, bei denen die Vorteile eines I/O Schedulers weniger wirksam sind.

- Es ist der am wenigsten invasive I/O Scheduler und kann bei Bedarf angepasst werden.

Ändern des Schedulers

Eine Änderung des I/O Schedulers kann die Leistung erhöhen oder verringern, je nachdem, ob der Scheduler dazu führt, dass mehr oder weniger I/O Anfragen in einer bestimmten Zeit abgeschlossen werden. Dies hängt weitgehend von Ihrer Workload, der Generierung des verwendeten Instance-Typs und dem Gerätetyp. Wenn Sie den verwendeten I/O-Scheduler ändern, empfehlen wir Ihnen, ein Tool wie iotop zu verwenden, um die I/O Leistung zu messen und festzustellen, ob die Änderung für Ihren Anwendungsfall von Vorteil ist.

Sie können den I/O Scheduler für ein Gerät mithilfe des folgenden Befehls anzeigen, der `nvme0n1` als Beispiel dient. Ersetzen Sie `nvme0n1` im folgenden Befehl mit dem Gerät in `/sys/block` Ihrer Instance.

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

Verwenden Sie den folgenden Befehl, um den I/O Scheduler für das Gerät einzurichten.

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

Verwenden Sie beispielsweise den folgenden Befehl, um den I/O Scheduler für ein *xvda* Gerät von noop bis `cfq` einzustellen.

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

Ändern Sie den Hostnamen Ihrer Instanz AL2

Wenn Sie eine Instance in einer privaten VPC starten, EC2 weist Amazon einen Gastbetriebssystem-Hostnamen zu. Die Art des Hostnamens, den Amazon EC2 zuweist, hängt von Ihren Subnetzeinstellungen ab. Weitere Informationen zu EC2 Hostnamen finden Sie unter Hostnamentypen für EC2 Amazon-Instances im EC2 Amazon-Benutzerhandbuch.

Ein typischer EC2 privater DNS-Name von Amazon für eine EC2 Instance, die für die Verwendung einer IP-basierten Benennung mit einer IPv4 Adresse konfiguriert ist`ip-12-34-56-78.us-west-2.compute.internal`, sieht ungefähr so aus:, wobei der Name aus der internen Domain, dem Service (in diesem Fall`compute`), der Region und einer Form der privaten IPv4 Adresse besteht. Teil dieses Hostnamens wird von der Shell-Anzeige gezeigt, wenn Sie sich bei der Instance

anmelden (z. B., `ip-12-34-56-78`). Jedes Mal, wenn Sie Ihre EC2 Amazon-Instance beenden und neu starten (es sei denn, Sie verwenden eine Elastic IP-Adresse), ändert sich die öffentliche IPv4 Adresse, ebenso wie Ihr öffentlicher DNS-Name, Ihr System-Hostname und Ihre Shell-Eingabeaufforderung.

> **Important**
>
> Diese Informationen gelten für Amazon Linux. Weitere Informationen zu anderen Verteilungen finden Sie in der jeweiligen Dokumentation.

Ändern des Systemhostnamens

Falls Sie für die IP-Adresse der Instance einen öffentlichen DNS-Namen registriert haben (z. B. `webserver.mydomain.com`), können Sie den Systemhostnamen so einstellen, dass sich die Instance als Teil dieser Domain identifiziert. Dadurch wird auch die Shell-Eingabeaufforderung so geändert, dass sie den ersten Teil dieses Namens anstelle des von AWS (z. B.) angegebenen Hostnamens anzeigt. `ip-12-34-56-78` Auch wenn Sie keinen öffentlichen DNS-Namen registriert haben, können Sie den Hostnamen ändern. Allerdings unterscheidet sich die Vorgehensweise ein wenig.

Damit Ihre Hostnamen-Aktualisierung fortbesteht, müssen Sie sicherstellen, dass die `preserve_hostname`-Cloud-Init-Einstellung auf `true` eingestellt ist. Sie können den folgenden Befehl ausführen, um diese Einstellung zu bearbeiten oder hinzuzufügen:

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

Wenn die `preserve_hostname`-Einstellung nicht aufgeführt ist, fügen Sie am Ende der Datei die folgende Textzeile hinzu:

```
preserve_hostname: true
```

Ändern Sie den Systemhostnamen wie folgt in einen öffentlichen DNS-Namen:

Führen Sie diese Schritte aus, falls Sie bereits einen öffentlichen DNS-Namen registriert haben.

1. • Für AL2: Verwenden Sie den hostnamectl Befehl, um Ihren Hostnamen so einzustellen, dass er den vollqualifizierten Domainnamen wiedergibt (z. B.**`webserver.mydomain.com`**).

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

- Für Amazon Linux AMI: Öffnen Sie auf der Instance die Konfigurationsdatei `/etc/sysconfig/network` in einem Texteditor Ihrer Wahl und ändern Sie den Eintrag `HOSTNAME` so, dass er den vollqualifizierten Domain-Namen wiederspiegelt (z. B. **`webserver.mydomain.com`**).

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

2. Starten Sie die Instance neu, damit der neue Hostname übernommen und angezeigt wird.

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

Alternativ können Sie den Neustart über die EC2 Amazon-Konsole durchführen (wählen Sie auf der Seite Instances die Instance aus und wählen Sie Instance state, Reboot instance).

3. Melden Sie sich bei der Instance an und überprüfen Sie, ob der Hostname aktualisiert wurde. Ihr Eintrag sollte den neuen Hostnamen bis zum ersten "." anzeigen, und der Befehl hostname sollte den vollqualifizierten Domain-Namen anzeigen.

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

Ändern Sie den Systemhostnamen wie folgt ohne einen öffentlichen DNS-Namen:

1.
- Für AL2: Verwenden Sie den hostnamectl Befehl, um Ihren Hostnamen so einzustellen, dass er dem gewünschten System-Hostnamen entspricht (z. B.**`webserver`**).

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

- Für Amazon Linux AMI: Öffnen Sie auf Ihrer Instance die Konfigurationsdatei `/etc/sysconfig/network` in einem Texteditor Ihrer Wahl und ändern Sie den Eintrag `HOSTNAME` so, dass er den gewünschten Systemhostnamen widerspiegelt (z. B. **`webserver`**).

```
HOSTNAME=webserver.localdomain
```

2. Öffnen Sie die Datei `/etc/hosts` in einem Texteditor Ihrer Wahl und ändern Sie den mit **`127.0.0.1`** beginnenden Eintrag so, dass er dem folgenden Beispiel entspricht, wobei Sie einen eigenen Hostnamen angeben.

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

3. Starten Sie die Instance neu, damit der neue Hostname übernommen und angezeigt wird.

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

   Alternativ können Sie den Neustart über die EC2 Amazon-Konsole durchführen (wählen Sie auf der Seite Instances die Instance aus und wählen Sie Instance state, Reboot instance).

4. Melden Sie sich bei der Instance an und überprüfen Sie, ob der Hostname aktualisiert wurde. Ihr Eintrag sollte den neuen Hostnamen bis zum ersten "." anzeigen, und der Befehl hostname sollte den vollqualifizierten Domain-Namen anzeigen.

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

Sie können auch mehr programmatische Lösungen implementieren, z. B. die Angabe von Benutzerdaten zur Konfiguration Ihrer Instance. Wenn Ihre Instance Teil einer Auto-Scaling-Gruppe ist, können Sie Lebenszyklus-Hooks verwenden, um Benutzerdaten festzulegen. Weitere Informationen finden Sie unter Ausführen von Befehlen auf Linux-Instances beim Start und Lebenszyklus-Hook für Instance-Start im AWS CloudFormation -Benutzerhandbuch.

Ändern der Shell-Anzeige ohne Auswirkungen auf den Hostnamen

Wenn Sie den Hostnamen für Ihre Instance nicht ändern möchten, aber einen sinnvolleren Systemnamen (wie) als den von AWS (z. B.**`webserver`**) angegebenen privaten Namen angezeigt haben möchten, `ip-12-34-56-78` können Sie die Shell-Prompt-Konfigurationsdateien so bearbeiten, dass Ihr System-Spitzname anstelle des Hostnamens angezeigt wird.

Lassen Sie die Shell-Anzeige wie folgt einen Hostspitznamen anzeigen:

1. Erstellen Sie eine Datei unter `/etc/profile.d`, die die Umgebungsvariable `NICKNAME` auf den Wert einstellt, den die Shell-Anzeige anzeigen soll. Führen Sie den folgenden Befehl aus, um als Systemspitznamen beispielsweise **`webserver`** festzulegen.

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

2. Öffnen Sie die Datei `/etc/bashrc` (Red Hat) oder `/etc/bash.bashrc` (Debian/Ubuntu) in Ihrem bevorzugten Texteditor (z. B. vim oder nano). Sie müssen sudo mit dem Editorbefehl verwenden, da `/etc/bashrc` und `/etc/bash.bashrc` Eigentum von `root` sind.
3. Bearbeiten Sie die Datei und ändern Sie die Shell-Anzeigenvariable (PS1) so, dass der Spitzname anstelle des Hostnamens angezeigt wird. Suchen Sie die folgende Zeile, in der die Shell-Anzeige in `/etc/bashrc` oder `/etc/bash.bashrc` festlegt wird (die Stelle und mehrere umgebende Zeilen werden im Folgenden angezeigt, um Kontext zu liefern. Suchen Sie die Zeile, die mit `[ "$PS1"` beginnt):

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

   Ändern Sie den Wert von \h (Symbol für `hostname`) in dieser Zeile auf den Wert der Variable `NICKNAME`.

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

4. (Optional) Führen Sie die folgenden Schritte aus, um die Titel von Shell-Fenstern auf den neuen Spitznamen einzustellen.

   a. Erstellen Sie eine Datei namens `/etc/sysconfig/bash-prompt-xterm`.

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

   b. Machen Sie die Datei mithilfe des folgenden Befehls ausführbar:

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

c. Öffnen Sie die Datei `/etc/sysconfig/bash-prompt-xterm` mit einem Texteditor Ihrer Wahl (z. B. vim oder nano). Sie müssen sudo mit dem Editor verwenden, da die Datei `/etc/sysconfig/bash-prompt-xterm` Eigentum von `root` ist.

d. Fügen Sie der Datei die folgende Zeile hinzu.

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

5. Melden Sie sich ab und wieder an, damit der neue Spitzname übernommen und angezeigt wird.

Ändern des Hostnamens auf anderen Linux-Bereitstellungen

Die Vorgehensweisen auf dieser Seite sind ausschließlich für die Verwendung mit Amazon Linux gedacht. Weitere Informationen zu anderen Linux-Bereitstellungen finden Sie in der jeweiligen Dokumentation und den folgenden Artikeln:

- Wie weise ich einer privaten EC2 Amazon-Instance, auf der RHEL 7 oder Centos 7 ausgeführt wird, einen statischen Hostnamen zu?

Richten Sie dynamisches DNS auf Ihrer Instance ein AL2

Wenn Sie eine EC2 Instance starten, werden ihr eine öffentliche IP-Adresse und ein öffentlicher DNS-Name (Domain Name System) zugewiesen, mit dem Sie sie über das Internet erreichen können. Diese öffentlichen Namen müssen relativ lang sein, um eindeutig zu bleiben, da sich sehr viele Hosts in der Amazon Web Services-Domain befinden. Ein typischer EC2 öffentlicher DNS-Name von Amazon sieht etwa so aus:`ec2-12-34-56-78.us-west-2.compute.amazonaws.com`, wobei der Name aus der Amazon Web Services Services-Domain, dem Service (in diesem Fall`compute`) AWS-Region, der und einer Form der öffentlichen IP-Adresse besteht.

Dynamische DNS-Services stellen innerhalb der Domain benutzerdefinierte DNS-Hostnamen zur Verfügung, die einprägsam sind und den Anwendungsfall des Hosts anzeigen. Einige dieser Services sind auch kostenlos. Sie können einen dynamischen DNS-Anbieter mit Amazon verwenden EC2 und die Instance so konfigurieren, dass die mit einem öffentlichen DNS-Namen verknüpfte IP-Adresse bei jedem Start der Instance aktualisiert wird. Sie können aus vielen verschiedenen Anbietern auswählen. Die genauen Details zur Auswahl eines Anbieters und der Registrierung eines Namens bei einem Anbieter würden den Rahmen dieses Leitfadens sprengen.

Um dynamisches DNS mit Amazon zu verwenden EC2

1. Registrieren Sie sich bei einem Serviceanbieter für ein dynamisches DNS und registrieren Sie bei diesem Anbieter einen öffentlichen DNS-Namen. Diese Vorgehensweise verwendet den kostenlosen Service von noip.com/free als Beispiel.
2. Konfigurieren des Aktualisierungsclient für das dynamische DNS. Sobald Sie über einen Serviceanbieter für ein dynamisches DNS und einen dort registrierten öffentlichen DNS-Namen verfügen, verknüpfen Sie den DNS-Namen mit der IP-Adresse einer Instance. Viele Anbieter (einschließlich noip.com) ermöglichen Ihnen, dies manuell von der Seite Ihres Benutzerkontos auf deren Website aus zu tun, aber viele unterstützen auch Aktualisierungsclients. Wenn auf Ihrer EC2 Instance ein Update-Client ausgeführt wird, wird Ihr dynamischer DNS-Eintrag jedes Mal aktualisiert, wenn sich die IP-Adresse ändert, wie dies nach einem Herunterfahren und einem Neustart der Fall ist. In diesem Beispiel wird der noip2-Client installiert, der mit dem von noip.com zur Verfügung gestellten Service zusammenarbeitet.

   a. Aktivieren Sie das EPEL-Repository (Extra Packages for Enterprise Linux), um Zugriff auf den `noip2` Client zu erhalten.

      > **Note**
      >
      > AL2 Auf Instanzen sind die GPG-Schlüssel und Repository-Informationen für das EPEL-Repository standardmäßig installiert. Weitere Informationen und den Download der neuesten Version dieses Pakets finden Sie unter https://fedoraproject.org/wiki/EPEL.

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

   b. Installieren Sie das Paket `noip`.

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

   c. Erstellen Sie die Konfigurationsdatei. Geben Sie Ihre Anmeldedaten an, wenn Sie dazu aufgefordert werden, und beantworten Sie die darauffolgenden Fragen, um den Client zu konfigurieren.

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

3. Aktivieren Sie den noip-Service.

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

4. Starten Sie den Service „noip“.

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

Dieser Befehl startet den Client, der die von Ihnen erstellte Konfigurationsdatei (`/etc/no-ip2.conf`) liest und die IP-Adresse für den von Ihnen ausgewählten öffentlichen DNS-Namen aktualisiert.

5. Überprüfen Sie, ob der Aktualisierungsclient die richtige IP-Adresse für den dynamischen DNS-Namen angegeben hat. Geben Sie den DNS-Datensätzen einige Minuten Zeit für die Aktualisierung und versuchen Sie dann, mithilfe von SSH eine Verbindung zwischen der Instance und dem anhand dieser Vorgehensweise konfigurierten öffentlichen DNS-Namen herzustellen.

Konfigurieren Sie Ihre Netzwerkschnittstelle mit ec2-net-utils für AL2

Amazon Linux 2 AMIs kann zusätzliche Skripts enthalten, die von AWS, so genannten ec2-net-utils, installiert wurden. Mit diesen Skripts kann die Konfiguration Ihrer Netzwerkschnittstellen optional automatisiert werden. Diese Skripte sind nur für verfügbar. AL2

> **Note**
>
> Für Amazon Linux 2023 generiert das `amazon-ec2-net-utils` Paket schnittstellenspezifische Konfigurationen im `/run/systemd/network` Verzeichnis. Weitere Informationen finden Sie unter Networking-Service im Benutzerhandbuch zu Amazon Linux 2023.

Verwenden Sie den folgenden Befehl, um das Paket zu installieren, AL2 falls es noch nicht installiert ist, oder aktualisieren Sie es, wenn es installiert ist und zusätzliche Updates verfügbar sind:

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

Die folgenden Komponenten sind Teil von ec2-net-utils:

udev-Regeln (`/etc/udev/rules.d`)

Identifiziert Netzwerkschnittstellen, wenn sie an eine laufende Instance angefügt, von ihr getrennt oder wieder angefügt werden, und stellt sicher, dass das Hotplug-Skript ausgeführt wird (`53-ec2-network-interfaces.rules`). Ordnet die MAC-Adresse einem Gerätenamen zu (`75-persistent-net-generator.rules`, der `70-persistent-net.rules` generiert).

Hotplug-Skript

Generiert eine Schnittstellenkonfigurationsdatei, die mit DHCP verwendet werden kann (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Generiert zudem eine Routing-Konfigurationsdatei (`/etc/sysconfig/network-scripts/route-ethN`).

DHCP-Skript

Wenn die Netzwerkschnittstelle einen neuen DHCP-Lease erhält, fragt dieses Skript die Instance-Metadaten nach Elastic IP-Adressen ab. Für jede Elastic IP-Adresse fügt es der Datenbank eine Regel für die Routing-Richtlinien hinzu, um sicherzustellen, dass für ausgehenden Datenverkehr die richtige Netzwerkschnittstelle verwendet wird. Sie fügt der Netzwerkschnittstelle darüber hinaus jede private IP-Adresse als sekundäre Adresse hinzu.

ec2ifup ethN (`/usr/sbin/`)

Erweitert die Funktionalität des ifup-Standardbefehls. Nachdem dieses Skript die Konfigurationsdateien `ifcfg-ethN` und `route-ethN` neu geschrieben hat, führt es den Befehl ifup aus.

ec2ifdown ethN (`/usr/sbin/`)

Erweitert die Funktionalität des ifdown-Standardbefehls. Nachdem dieses Skript sämtliche Regeln für die Netzwerkschnittstelle aus der Datenbank für die Routing-Richtlinien entfernt hat, führt es den Befehl ifdown aus.

ec2ifscan (`/usr/sbin/`)

Führt eine Prüfung auf unkonfigurierte Netzwerkschnittstellen durch und konfiguriert sie.

Dieses Skript ist in der ersten Version von ec2-net-utils nicht verfügbar.

Verwenden Sie den folgenden Befehl, um sämtliche Konfigurationsdateien aufzulisten, die von ec2-net-utils generiert wurden:

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

Um die Automatisierung zu deaktivieren, können Sie `EC2SYNC=no` der entsprechenden Datei `ifcfg-ethN` hinzufügen. Verwenden Sie z. B. den folgenden Befehl, um die Automatisierung für die Schnittstelle eth1 zu deaktivieren:

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

Zum vollständigen Deaktivieren der Automatisierung können Sie das Paket mithilfe des folgenden Befehls entfernen:

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

Vom Benutzer bereitgestellte Kernel

Wenn Sie einen benutzerdefinierten Kernel für Ihre EC2 Amazon-Instances benötigen, können Sie mit einem AMI beginnen, das Ihren Wünschen sehr nahe kommt, den benutzerdefinierten Kernel auf Ihrer Instance kompilieren und den Bootloader so aktualisieren, dass er auf den neuen Kernel verweist. Dieser Prozess variiert je nach Virtualisierungstyp, der von Ihrem AMI verwendet wird. Weitere Informationen finden Sie unter Linux-AMI-Virtualisierungstypen im EC2 Amazon-Benutzerhandbuch.

Inhalt

HVM AMIs (GRUB)

HVM-Instance-Volumes werden wie echte physische Datenträger behandelt. Der Startvorgang ähnelt dem Vorgang eines Bare-Metal-Betriebssystems mit einem partitionierten Datenträger und Bootloader, sodass die Verwendung mit allen derzeit unterstützten Linux-Distributionen möglich ist. Der gebräuchlichste Bootloader ist GRUB oder. GRUB2

Standardmäßig sendet GRUB seine Ausgabe nicht an die Instance-Konsole, da dies zu einer zusätzlichen Startverzögerung führt. Weitere Informationen finden Sie unter Ausgabe der Instance-Konsole im EC2 Amazon-Benutzerhandbuch. Wenn Sie einen benutzerdefinierten Kernel installieren, sollten Sie erwägen, die GRUB-Ausgabe zu aktivieren.

Es ist nicht erforderlich, einen Fallback-Kernel anzugeben. Es empfiehlt sich jedoch die Verwendung eines Fallbacks, wenn Sie einen neuen Kernel testen. In GRUB kann dann ein Fallback auf einen anderen Kernel durchgeführt werden, falls der neue Kernel ausfällt. Bei Vorhandensein eines Fallback-Kernels kann die Instance auch dann gestartet werden, wenn der neue Kernel nicht gefunden werden kann.

Das Legacy-GRUB für Amazon Linux verwendet`/boot/grub/menu.lst`. GRUB2 für AL2 Anwendungen`/etc/default/grub`. Weitere Informationen zum Aktualisieren des Standardkernels im Bootloader finden Sie in der Dokumentation für die Linux-Distribution.

Paravirtuell AMIs (PV-GRUB)

AMIs die paravirtuelle (PV) Virtualisierung verwenden, verwenden während des Startvorgangs ein System namens PV-GRUB. PV-GRUB ist ein Paravirtual-Bootloader, bei dem eine gepatchte Version von GNU GRUB 0.97 ausgeführt wird. Wenn Sie eine Instance starten, startet PV-GRUB den Bootprozess und führt dann das Chain Loading für den Kernel durch, der in der Datei `menu.lst` Ihres Images angegeben ist.

PV-GRUB erkennt standardmäßige `grub.conf`- oder `menu.lst`-Befehle, sodass alle derzeit unterstützten Linux-Distributionen verwendet werden können. Für ältere Distributionen, z. B. Ubuntu 10.04 LTS, Oracle Enterprise Linux oder CentOS 5.x, ist ein spezielles Kernel-Paket vom Typ „ec2“ oder „xen“ erforderlich. Bei neueren Distributionen sind die erforderlichen Treiber im Kernel-Standardpaket enthalten.

Die meisten modernen Paravirtuals AMIs verwenden standardmäßig eine PV-GRUB-AKI (einschließlich aller paravirtuellen Linux-Dateien, die im Schnellstartmenü des Amazon EC2 Launch Wizard AMIs verfügbar sind). Sie müssen also keine zusätzlichen Schritte unternehmen, um einen anderen Kernel auf Ihrer Instance zu verwenden, vorausgesetzt, der Kernel, den Sie verwenden möchten, ist mit Ihrer Distribution kompatibel. Der beste Ansatz zur Ausführung eines benutzerdefinierten Kernels auf Ihrer Instance besteht darin, mit einem AMI zu beginnen, das Ihren Anforderungen am ehesten entspricht. Kompilieren Sie den benutzerdefinierten Kernel dann auf Ihrer Instance und ändern Sie die Datei `menu.lst`, um den Startvorgang mit diesem Kernel durchzuführen.

Sie können überprüfen, ob das Kernel-Image für ein AMI ein PV-GRUB-AKI ist. Führen Sie den folgenden Befehl describe-images aus (ersetzt Ihre Kernel-Image-ID) und überprüfen Sie, ob das `Name`-Feld mit `pv-grub` beginnt:

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

Inhalt

Einschränkungen von PV-GRUB

Für PV-GRUB gelten die folgenden Einschränkungen:

- Es ist nicht möglich, die 64-Bit-Version von PV-GRUB zu verwenden, um einen 32-Bit-Kernel zu starten (und umgekehrt).
- Bei Verwendung eines PV-GRUB-AKI können Sie kein Amazon Ramdisk Image (ARI) angeben.
- AWS hat getestet und verifiziert, dass PV-GRUB mit den folgenden Dateisystemformaten funktioniert: EXT2,,, JFS EXT3 EXT4, XFS und ReiserFS. Andere Dateisystemformate funktionieren unter Umständen nicht.
- PV-GRUB kann Kernel starten, die mit den Komprimierungsformaten gzip, bzip2, lzo und xz komprimiert wurden.
- Cluster unterstützen oder benötigen PV-GRUB AMIs nicht, da sie die vollständige Hardwarevirtualisierung (HVM) verwenden. Während Paravirtual-Instances zum Starten PV-GRUB verwenden, werden HVM-Instance-Volumes wie echte Datenträger behandelt. Der Startvorgang ähnelt dem Startvorgang eines Bare-Metal-Betriebssystems mit einem partitionierten Datenträger und Bootloader.
- Die PV-GRUB-Versionen 1.03 und früher weisen keine Unterstützung für die GPT-Partitionierung auf, sondern nur für die MBR-Partitionierung.
- Wenn Sie planen, einen Logical Volume Manager (LVM) für Volumes Amazon Elastic Block Store (Amazon EBS) zu verwenden, benötigen Sie eine separate Boot-Partition außerhalb des LVM. Anschließend können Sie mit dem LVM logische Volumes erstellen.

Konfigurieren Sie GRUB für paravirtuell AMIs

Zum Starten von PV-GRUB muss im Image die GRUB-Datei `menu.lst` enthalten sein. Der am häufigsten verwendete Speicherort für diese Datei ist `/boot/grub/menu.lst`.

Unten ist ein Beispiel für die Konfigurationsdatei `menu.lst` zum Starten eines AMI mit einem PV-GRUB-AKI angegeben. In diesem Beispiel können Sie zwischen zwei Kernel-Einträgen wählen: Amazon Linux 2018.03 (ursprünglicher Kernel für dieses AMI) und Vanilla Linux 4.16.4 (neuere Version des Vanilla Linux-Kernels von https://www.kernel.org/). Der Vanilla-Eintrag wurde aus dem Originaleintrag für dieses AMI kopiert und die Pfade `kernel` und `initrd` wurden auf die neuen Speicherorte aktualisiert. Mit dem Parameter `default 0` wird für den Bootloader auf den ersten Eintrag verwiesen, der sichtbar ist (in diesem Fall der Vanilla-Eintrag), und mit dem Parameter `fallback 1` wird für den Bootloader auf den nächsten Eintrag verwiesen, falls beim Starten des ersten Eintrags ein Problem auftritt.

```
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
```

Es ist nicht erforderlich, in Ihrer Datei `menu.lst` einen Fallback-Kernel anzugeben. Wir empfehlen Ihnen aber die Verwendung eines Fallbacks, wenn Sie einen neuen Kernel testen. In PV-GRUB kann dann ein Fallback auf einen anderen Kernel durchgeführt werden, falls der neue Kernel ausfällt. Bei Vorhandensein eines Fallback-Kernels kann die Instance auch dann gestartet werden, wenn der neue Kernel nicht gefunden werden kann.

PV-GRUB prüft die folgenden Speicherorte auf das Vorhandensein von `menu.lst` und verwendet das erste Vorkommen der Datei:

- `(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`

Beachten Sie, dass mit PV-GRUB 1.03 und früher nur einer der ersten beiden Speicherorte der Liste geprüft wird.

Amazon PV-GRUB-Kernel-Image IDs

PV-GRUB AKIs sind in allen EC2 Amazon-Regionen mit Ausnahme des asiatisch-pazifischen Raums (Osaka) erhältlich. Es gibt sowohl 32-Bit AKIs - als auch 64-Bit-Architekturtypen. Die meisten modernen AMIs Geräte verwenden standardmäßig ein PV-GRUB-AKI.

Wir empfehlen Ihnen, immer die aktuelle Version des PV-GRUB-AKI zu nutzen, da nicht alle Versionen des PV-GRUB-AKI mit allen Instance-Typen kompatibel sind. Verwenden Sie den folgenden Befehl describe-images, um eine Liste der AKIs PV-GRUB-Dateien für die aktuelle Region abzurufen:

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

PV-GRUB ist das einzige AKI, das in der Region `ap-southeast-2` verfügbar ist. Stellen Sie sicher, dass für AMIs, die Sie in diese Region kopieren möchten, eine Version von PV-GRUB verwendet wird, die in dieser Region verfügbar ist.

Im Folgenden sind die aktuellen AKI für jede Region aufgeführt. IDs Registrieren Sie sich neu AMIs mit einem hd0-AKI.

> **Note**
>
> Aus AKIs Gründen der Abwärtskompatibilität bieten wir weiterhin hd00 in Regionen an, in denen sie zuvor verfügbar waren.

ap-northeast-1, Asia Pacific (Tokyo)

Image-ID	Name des Images
aki-f975a998	pv-grub-hd0_1.05-i386.gz
aki-7077ab11	pv-grub-hd0_1.05-x86_64.gz

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

Image-ID	Name des Images
aki-17a40074	pv-grub-hd0_1.05-i386.gz
aki-73a50110	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-2, Asia Pacific (Sydney)

Image-ID	Name des Images
aki-ba5665d9	pv-grub-hd0_1.05-i386.gz
aki-66506305	pv-grub-hd0_1.05-x86_64.gz

eu-central-1, Europe (Frankfurt)

Image-ID	Name des Images
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1, Europe (Ireland)

Image-ID	Name des Images
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz

Image-ID	Name des Images
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1, South America (São Paulo)

Image-ID	Name des Images
aki-7cd34110	pv-grub-hd0_1.05-i386.gz
aki-912fbcfd	pv-grub-hd0_1.05-x86_64.gz

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

Image-ID	Name des Images
aki-04206613	pv-grub-hd0_1.05-i386.gz
aki-5c21674b	pv-grub-hd0_1.05-x86_64.gz

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

Image-ID	Name des Images
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

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

Image-ID	Name des Images
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2, US West (Oregon)

Image-ID	Name des Images
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

Aktualisieren von PV-GRUB

Wir empfehlen Ihnen, immer die aktuelle Version des PV-GRUB-AKI zu nutzen, da nicht alle Versionen des PV-GRUB-AKI mit allen Instance-Typen kompatibel sind. Ältere Versionen von PV-GRUB sind ebenfalls nicht in allen Regionen verfügbar. Beim Kopieren eines AMI, für das eine ältere Version verwendet wird, in eine Region, von der diese Version nicht unterstützt wird, gilt daher Folgendes: Das Starten von Instances, die über dieses AMI gestartet werden, ist erst möglich, wenn Sie das Kernel-Image aktualisieren. Verwenden Sie die folgenden Vorgehensweisen, um die PV-GRUB-Version Ihrer Instance zu überprüfen und ggf. zu aktualisieren.

So überprüfen Sie Ihre PV-GRUB-Version

1. Ermitteln Sie die Kernel-ID für Ihre Instance.

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

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

   Die Kernel-ID für diese Instance lautet `aki-70cb0e10`.

2. Zeigen Sie die Versionsinformationen für diese Kernel-ID an.

```
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"
        }
    ]
}
```

Dieses Kernel-Image hat die Version PV-GRUB 1.05. Falls Sie nicht die aktuelle PV-GRUB-Version nutzen (wie unter Amazon PV-GRUB-Kernel-Image IDs gezeigt), sollten Sie das Image mit den unten angegebenen Schritten aktualisieren.

So aktualisieren Sie Ihre PV-GRUB-Version

Wenn für Ihre Instance eine ältere Version von PV-GRUB verwendet wird, sollten Sie das Update auf die aktuelle Version durchführen.

1. Ermitteln Sie das aktuelle PV-GRUB-AKI für Ihre Region und Prozessorarchitektur anhand von Amazon PV-GRUB-Kernel-Image IDs.
2. Halten Sie Ihre Instance an. Ihre Instance muss angehalten werden, damit das verwendete Kernel-Image geändert werden kann.

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

3. Ändern Sie das Kernel-Image, das für Ihre Instance verwendet wird.

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

4. Starten Sie Ihre Instance neu.

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

AL2 AMI-Release-Benachrichtigungen

Um benachrichtigt zu werden, wenn neue Amazon AMIs Linux-Versionen veröffentlicht werden, können Sie ein Abonnement über Amazon SNS abschließen.

Informationen zum Abonnieren von Benachrichtigungen für AL2 023 finden Sie unter Empfangen von Benachrichtigungen über neue Updates im Amazon Linux 2023-Benutzerhandbuch.

> **Note**
>
> Der Standard-Support für AL1 endete am 31. Dezember 2020. Die Phase des AL1 Wartungssupports endete am 31. Dezember 2023. Weitere Informationen zur AL1 EOL und zum Wartungssupport finden Sie im Blogbeitrag Update on Amazon Linux AMI end-of-life.

So abonnieren Sie Amazon Linux-Benachrichtigungen

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen die Region auswählen, in der die SNS-Benachrichtigung, die Sie abonnieren, erstellt wurde.
3. Wählen Sie im Navigationsbereich Subscriptions und Create subscription aus.
4. Führen Sie im Dialogfeld Create subscription die folgenden Schritte aus:
   a. [AL2]Kopieren Sie für Topic ARN den folgenden Amazon-Ressourcennamen (ARN): **`arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates`**.
   b. [Amazon Linux]Kopieren Sie für Topic ARN den folgenden Amazon-Ressourcennamen (ARN): **`arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates`**.
   c. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
   d. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.
   e. Wählen Sie Create subscription.
5. Sie erhalten eine Bestätigungs-E-Mail mit dem Betreff „AWS Benachrichtigung — Abonnementbestätigung“. Öffnen Sie die E-Mail und wählen Sie Confirm subscription aus, um Ihr Abonnement abzuschließen.

Wann immer diese veröffentlicht AMIs werden, senden wir Benachrichtigungen an die Abonnenten des entsprechenden Themas. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So melden Sie sich von den Amazon Linux-Benachrichtigungen ab

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.

2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen die Region verwenden, in der die SNS-Benachrichtigung erstellt wurde.
3. Wählen Sie im Navigationsbereich Subscriptions (Abonnements) und dann das Abonnement aus. Klicken Sie dann auf Actions (Aktionen) und Delete subscriptions (Abonnements löschen).
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Amazon Linux-AMI SNS-Nachrichtenformat

Das Schema für die SNS-Nachricht lautet wie folgt.

```
{
    "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"
]
}
```

Konfigurieren Sie die MATE-Desktop-Verbindung AL2

Die MATE-Desktop-Umgebung ist vorinstalliert und AMIs mit der folgenden Beschreibung vorkonfiguriert:

".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)."

Die Umgebung bietet eine intuitive grafische Benutzeroberfläche für die Verwaltung von AL2 - Instances mit minimaler Verwendung der Befehlszeile. Die Schnittstelle verwendet grafische Darstellungen, wie z. B. Symbole, Fenster, Symbolleisten, Ordner, Hintergrundbilder und Desktop-Widgets. Integrierte, GUI-basierte Tools sind zur Ausführung allgemeiner Aufgaben verfügbar. Es gibt beispielsweise Tools zum Hinzufügen und Entfernen von Software, zum Anwenden von Updates, zum Organisieren von Dateien, zum Starten von Programmen und zum Überwachen des Systemstatus.

> **Important**
>
> `xrdp` ist die im AMI gebündelte Remote-Desktop-Software. Standardmäßig verwendet `xrdp` ein selbstsigniertes TLS-Zertifikat, um Remotedesktopsitzungen zu verschlüsseln. AWS Weder die Entwickler noch die `xrdp` Entwickler empfehlen, selbstsignierte Zertifikate in der Produktion zu verwenden. Beziehen Sie stattdessen ein Zertifikat von einer entsprechenden Zertifizierungsstelle (CA) und installieren Sie es auf Ihren Instances. Weitere Informationen über die TLS-Konfiguration finden Sie in TLS-Sicherheitsebene auf der `xrdp`-Wiki.

> **Note**
>
> Wenn Sie lieber einen Virtual Network Computing (VNC) -Service anstelle von xrdp verwenden möchten, lesen Sie den Artikel Wie installiere ich eine GUI auf meiner EC2 Amazon-Instance, auf der das AL2 AWS Knowledge Center ausgeführt wird?

Voraussetzung

Um die in diesem Thema aufgeführten Befehle auszuführen, müssen Sie AWS Command Line Interface (AWS CLI) oder AWS Tools for Windows PowerShell installieren und Ihr AWS Profil konfigurieren.

Optionen

1. Installation des AWS CLI — Weitere Informationen finden Sie unter Installation AWS CLI und Grundlagen der Konfiguration im AWS Command Line Interface Benutzerhandbuch.
2. Installieren Sie die Tools für Windows PowerShell — Weitere Informationen finden Sie im AWS -Tools für PowerShell Benutzerhandbuch unter Installation von AWS Tools for Windows PowerShell und Gemeinsam genutzte Anmeldeinformationen.

> **Tip**
>
> Als Alternative zur vollständigen Installation von können Sie eine browserbasierte AWS CLI, vorauthentifizierte Shell verwenden AWS CloudShell, die direkt von der aus gestartet wird.

AWS-Managementkonsole Vergewissern Sie sich AWS-Regionen, dass der Support in der Region, in der Sie arbeiten, verfügbar ist.

Konfigurieren Sie die RDP-Verbindung

Befolgen Sie diese Schritte, um eine Remote Desktop Protocol (RDP) -Verbindung von Ihrem lokalen Computer zu einer AL2 -Instance einzurichten, auf der die MATE-Desktop-Umgebung ausgeführt wird.

1. Um die ID des AMIs abzurufen AL2 , für das MATE im AMI-Namen enthalten ist, können Sie den Befehl describe-images in Ihrem lokalen Befehlszeilentool verwenden. Wenn Sie die Befehlszeilentools nicht installiert haben, können Sie die folgende Abfrage direkt von einer AWS CloudShell Sitzung aus ausführen. Informationen zum Starten einer Shell-Sitzung CloudShell finden Sie unter Erste Schritte mit AWS CloudShell. Von der EC2 Amazon-Konsole aus können Sie das im MATE enthaltene AMI finden, indem Sie eine Instance starten und dann `MATE` in die AMI-Suchleiste eingeben. Der AL2 Quick Start mit vorinstalliertem MATE wird in den Suchergebnissen angezeigt.

```
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"
    ]
]
```

   Wählen Sie das AMI, das für Ihre Verwendung geeignet ist.

2. Starten Sie eine EC2 Instance mit dem AMI, das Sie im vorherigen Schritt gefunden haben. Konfigurieren Sie die Sicherheitsgruppe so, dass eingehender TCP-Datenverkehr an Port 3389

zugelassen wird. Weitere Informationen über das Konfigurieren von Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihre VPC. Mit dieser Konfiguration können Sie einen RDP-Client verwenden, um eine Verbindung mit der Instance herzustellen.

3. Stellen Sie über SSH eine Verbindung mit der Instance her.
4. Aktualisieren Sie die Software und den Kernel auf der Instance.

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

Starten Sie nach Abschluss der Aktualisierung die Instance neu, damit die neuesten Pakete und Bibliotheken aus dem Update genutzt werden. Kernel-Updates werden erst nach einem Neustart des Systems geladen.

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

5. Stellen Sie eine neue Verbindung zur Instance her und führen Sie den folgenden Befehl auf Ihrer Linux-Instance aus, um das Passwort für `ec2-user` festzulegen.

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

6. Installieren Sie das Zertifikat und den Schlüssel.

Wenn Sie bereits über ein Zertifikat und einen Schlüssel verfügen, kopieren Sie diese in das Verzeichnis `/etc/xrdp/` wie folgt:

- Zertifikat – `/etc/xrdp/cert.pem`
- Schlüssel: `/etc/xrdp/key.pem`

Wenn Sie kein Zertifikat und keinen Schlüssel haben, verwenden Sie den folgenden Befehl, um sie im `/etc/xrdp`-Verzeichnis zu generieren.

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

> **Note**
>
> Dieser Befehl generiert ein Zertifikat, das 365 Tage gültig ist.

7. Öffnen Sie einen RDP-Client auf dem Computer, von dem aus Sie eine Verbindung zur Instance herstellen werden (z. B. Remote-Desktop-Verbindung auf einem Computer mit Microsoft Windows). Geben Sie `ec2-user` als Benutzernamen ein und geben Sie das Passwort ein, das Sie im vorherigen Schritt festgelegt haben.

Zur Deaktivierung **`xrdp`** auf Ihrer EC2 Amazon-Instance

Sie können `xrdp` jederzeit ausschalten, indem Sie einen der folgenden Befehle auf Ihrer Linux-Instance ausführen. Die folgenden Befehle wirken sich nicht auf Ihre Fähigkeit aus, MATE mit einem X11-Server zu verwenden.

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

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

Zur Aktivierung **`xrdp`** auf Ihrer EC2 Amazon-Instance

Um die Instance erneut zu aktivieren, `xrdp` sodass Sie eine Verbindung zu Ihrer AL2 Instance herstellen können, auf der die MATE-Desktop-Umgebung ausgeführt wird, führen Sie einen der folgenden Befehle auf Ihrer Linux-Instance aus.

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

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

AL2 Anleitungen

Die folgenden Tutorials zeigen Ihnen, wie Sie allgemeine Aufgaben mit laufenden EC2 Amazon-Instances ausführen AL2. Video-Tutorials finden Sie unter AWS Lehrvideos und Übungen.

Anleitungen für AL2 023 finden Sie unter Tutorials im Amazon Linux 2023 User Guide.

Lernprogramme

- Tutorial: Installieren Sie einen LAMP-Server auf AL2
- Tutorial: Konfiguration SSL/TLS am AL2
- Tutorial: Hosten Sie einen WordPress Blog auf AL2

Tutorial: Installieren Sie einen LAMP-Server auf AL2

Die folgenden Verfahren helfen Ihnen bei der Installation eines Apache-Webservers mit PHP- und MariaDB-Unterstützung (ein von der Community entwickelter Fork von MySQL) auf Ihrer AL2 Instance (manchmal auch LAMP-Webserver oder LAMP-Stack genannt). Sie können diesen Server dazu verwenden, eine statische Website zu hosten oder eine dynamische PHP-Anwendung bereitzustellen, die Informationen aus einer Datenbank liest und in diese schreibt.

> **Important**
>
> Dieses Tutorial funktioniert nicht, wenn Sie versuchen, einen LAMP-Webserver auf einer anderen Verteilung, wie z. B. Ubuntu oder Red Hat Enterprise Linux, einzurichten. Informationen zu AL2 023 finden Sie unter Installieren eines LAMP-Servers auf 023. AL2 Informationen zu Ubuntu finden Sie in der folgenden Dokumentation der Ubuntu-Community: ApacheMy SQLPHP. Andere Verteilungen finden Sie in der jeweiligen Dokumentation.

Option: Abschließen dieses Tutorials mit Automation

Um dieses Tutorial mit AWS Systems Manager Automatisierung anstelle der folgenden Aufgaben abzuschließen, führen Sie das AWS Dokument Docs-Install ALAMPServer — AL2 Automation aus.

Aufgaben

- Schritt 1: Vorbereiten des LAMP-Servers
- Schritt 2: Testen Ihres Lamp-Servers
- Schritt 3: Sichern des Datenbankservers
- Schritt 4: (Optional) Installieren phpMyAdmin
- Fehlerbehebung
- Verwandte Themen

Schritt 1: Vorbereiten des LAMP-Servers

Voraussetzungen

- In dieser Anleitung wird davon ausgegangen, dass Sie bereits eine neue Instanz mit einem öffentlichen DNS-Namen gestartet haben AL2, der über das Internet erreichbar ist. Weitere

Informationen finden Sie unter Launch an Instance im EC2 Amazon-Benutzerhandbuch. Außerdem müssen Sie Ihre Sicherheitsgruppe so konfiguriert haben, dass Verbindungen über SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) erlaubt sind. Weitere Informationen zu diesen Voraussetzungen finden Sie unter Sicherheitsgruppenregeln im EC2 Amazon-Benutzerhandbuch.

- Mit dem folgenden Verfahren wird die neueste PHP-Version installiert AL2, die derzeit verfügbar istphp8.2. Falls Sie andere PHP-Anwendungen als die in diesem Tutorial beschriebenen verwenden möchten, prüfen Sie ihre Kompatibilität mit php8.2.

Vorbereiten des LAMP-Servers

1. Verbinden Sie sich mit der Instance.
2. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus. Dieser Vorgang kann einige Minuten dauern. Es ist jedoch wichtig, sicherzustellen, dass Sie über die aktuellen Sicherheitsaktualisierungen und Fehlerbehebungen verfügen.

   Mit der Option -y werden die Updates installiert, ohne um Bestätigung zu bitten. Wenn Sie die Aktualisierungen vor der Installation überprüfen möchten, können Sie diese Option auslassen.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```
3. Installieren Sie die Amazon-Linux-Extras-Repositorys vom Typ mariadb10.5, um die aktuelle Version des MariaDB-Pakets zu erhalten.

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

   Wenn die Fehlermeldung sudo: amazon-linux-extras: command not found angezeigt wird, wurde Ihre Instance nicht mit einem Amazon Linux 2-AMI; gestartet (möglicherweise verwenden Sie stattdessen das Amazon Linux AMI). Sie können Ihre Version von Amazon Linux mit dem folgenden Befehl anzeigen.

   ```
   cat /etc/system-release
   ```
4. Installieren Sie die php8.2 Amazon Linux Extras-Repositorys, um die neueste Version des PHP Pakets für AL2 zu erhalten.

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

5. Nachdem Ihre Instance nur auf dem neuesten Stand ist, können Sie die Softwarepakete für Apache-Webserver, MariaDB und PHP installieren. Verwenden Sie den Befehl „yum install“, um mehrere Softwarepakete und alle zugehörigen Abhängigkeiten gleichzeitig zu installieren.

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

   Sie können die aktuellen Versionen dieser Pakete mit dem folgenden Befehl anzeigen:

   ```
   yum info package_name
   ```

6. Starten Sie den Apache-Webserver.

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

7. Konfigurieren Sie den Apache-Webserver mit dem Befehl systemctl so, dass er bei jedem Systemstart startet.

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

   Mit folgendem Befehl können Sie prüfen, ob der Befehl httpd ausgeführt wird:

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

8. Fügen Sie eine Sicherheitsregel hinzu, um eingehende HTTP-Verbindungen (Port 80) auf Ihre Instance zuzulassen, wenn Sie dies nicht bereits getan haben. Standardmäßig wurde während der Initialisierung eine ***N*** Launch-Wizard-Sicherheitsgruppe für Ihre Instance eingerichtet. Diese Gruppe enthält eine einzige Regel, um SSH-Verbindungen zuzulassen.

   a. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

   b. Wählen Sie Instances und wählen Sie Ihre Instance aus.

   c. Zeigen Sie auf der Registerkarte Sicherheit die Regeln für eingehenden Datenverkehr an. Sie sollten die folgende Regel sehen:

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

> **Warning**
>
> `0.0.0.0/0`Durch Verwenden können alle IPv4 Adressen über SSH auf Ihre Instance zugreifen. Dies ist zwar für kurze Zeit in einer Testumgebung akzeptabel, aber für Produktionsumgebungen sehr unsicher. Für die Produktion wird nur eine bestimmte IP-Adresse bzw. ein bestimmter Adressbereich für den Zugriff auf Ihre Instance autorisiert.

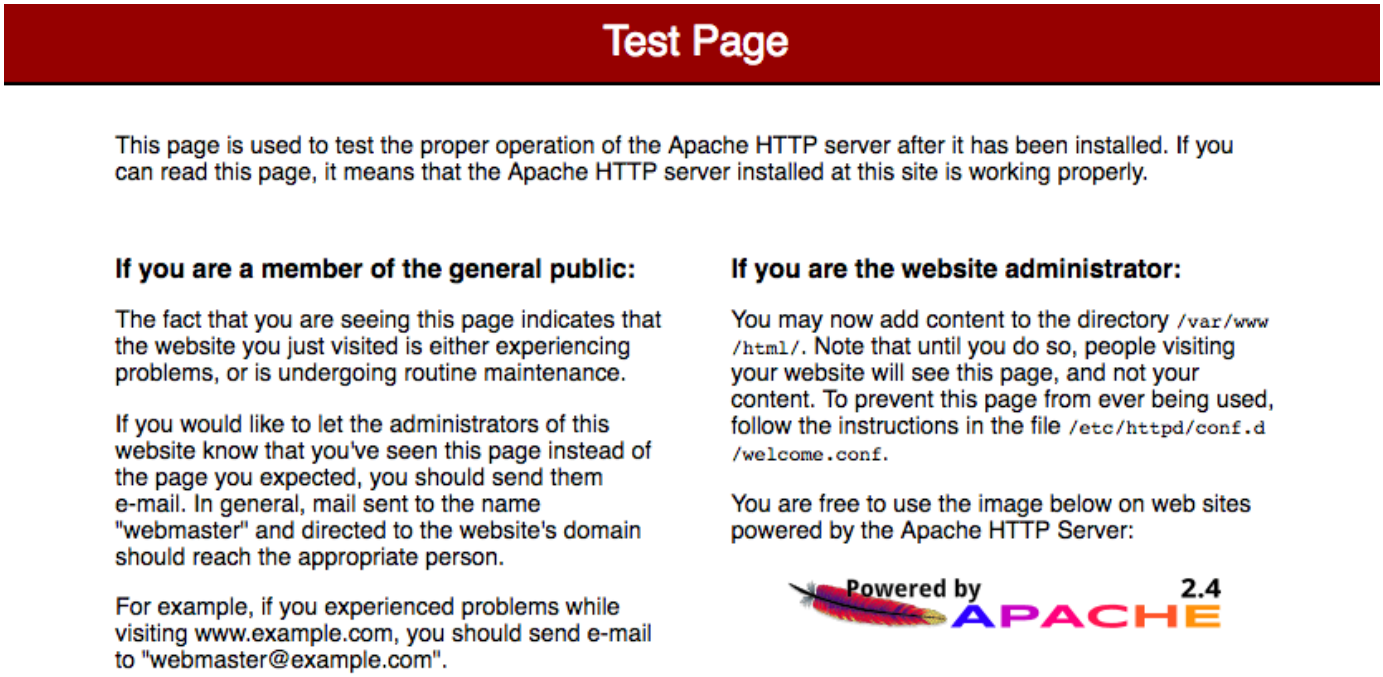
d. Wählen Sie den Link für die Sicherheitsgruppe aus. Fügen Sie mithilfe der Verfahren unter Regeln zu einer Sicherheitsgruppe hinzufügen eine neue Sicherheitsregel für eingehenden Datenverkehr mit den folgenden Werten hinzu:

   - Typ: HTTP
   - Protocol (Protokoll): TCP
   - Portbereich: 80
   - Quelle: Benutzerdefiniert

9. Testen Sie Ihren Webserver. Geben Sie in einen Web-Browser die öffentliche DNS-Adresse (oder die öffentliche IP-Adresse) Ihrer Instance ein. Wenn keine Inhalte in `/var/www/html` vorhanden sind, sollte die Testseite von Apache angezeigt werden. Sie können das öffentliche DNS für Ihre Instance über die EC2 Amazon-Konsole abrufen (überprüfen Sie die Spalte Öffentliche DNS; wenn diese Spalte ausgeblendet ist, wählen Sie Spalten ein-/ausblenden (das zahnradförmige Symbol) und wählen Sie Public DNS).

   Stellen Sie sicher, dass die Sicherheitsgruppe für die Instance eine Regel enthält, die HTTP-Datenverkehr auf Port 80 zulässt. Weitere Informationen finden Sie unter Regeln zur Sicherheitsgruppe hinzufügen.

   > **Important**
   >
   > Wenn Sie nicht Amazon Linux verwenden, müssen Sie möglicherweise auch die Firewall auf Ihrer Instance konfigurieren, um diese Verbindungen zu erlauben. Weitere Informationen zum Konfigurieren der Firewall finden Sie in der Dokumentation für Ihre spezifische Verteilung.



Der Apache-Befehl httpd gilt für Dateien, die in einem Verzeichnis gespeichert sind, das als Apache-Dokumenten-Stammverzeichnis bezeichnet wird. Das Amazon Linux-Apache-Dokumenten-Stammverzeichnis ist `/var/www/html`, das standardmäßig Eigentum des Stammverzeichnisses ist.

Damit das `ec2-user`-Konto Dateien in diesem Verzeichnis bearbeiten kann, müssen Sie die Eigentümerschaft und die Berechtigungen des Verzeichnisses ändern. Es gibt viele Möglichkeiten, um diese Aufgabe zu erfüllen. In diesem Tutorial fügen Sie `ec2-user` zur `apache`-Gruppe hinzu, geben der `apache`-Gruppe Eigentümerschaft über das Verzeichnis `/var/www` und weisen der Gruppe Schreibberechtigungen zu.

So richten Sie Dateiberechtigungen ein

1. Fügen Sie Ihren Benutzer (in diesem Fall `ec2-user`) zu der `apache`-Gruppe hinzu.

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

2. Melden Sie sich ab und anschließend wieder an, um die neue Gruppe auszuwählen, und verifizieren Sie dann Ihre Mitgliedschaft.

a. Melden Sie sich ab (Sie können den Befehl exit verwenden oder das Terminal-Fenster schließen):

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

b. Ihre Mitgliedschaft in der apache-Gruppe zu verifizieren, stellen Sie erneut die Verbindung zu Ihrer Instance her und führen Sie anschließend den folgenden Befehl aus:

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

3. Übertragen Sie die Eigentümerschaft der Datei /var/www und ihrer Inhalte auf die apache-Gruppe.

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

4. Um Schreibberechtigungen für die Gruppe hinzuzufügen und die Gruppen-ID für zukünftige Unterverzeichnisse einzurichten, ändern Sie die Verzeichnisberechtigungen von /var/www und deren Unterverzeichnisse.

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

5. Um Schreibberechtigungen für die Gruppe hinzuzufügen, ändern Sie die Dateiberechtigungen von /var/www und deren Unterverzeichnisse rekursiv.

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

Jetzt kann ec2-user (und jedes zukünftige Mitglied der apache-Gruppe) im Dokumenten-Stammverzeichnis von Apache Dateien hinzufügen, löschen und bearbeiten. Auf diese Weise können Sie Inhalte hinzufügen, beispielsweise eine statische Website oder eine PHP-Anwendung.

So sichern Sie Ihren Webserver (optional)

Ein Webserver, auf dem HTTP ausgeführt wird, bietet keine Transportsicherheit für die gesendeten oder empfangenen Daten. Wenn Sie über einen Webbrowser eine Verbindung zu einem HTTP-Server herstellen, sind URLs die von Ihnen besuchten Daten, der Inhalt der Webseiten, die Sie erhalten, und die Inhalte (einschließlich Kennwörter) aller HTML-Formulare, die Sie einreichen,

für Lauscher überall im Netzwerkpfad sichtbar. Die beste Methode, Ihren Webserver abzusichern, besteht darin, Unterstützung für HTTPS (HTTP Secure) zu installieren, wodurch Ihre Daten mit der SSL/TLS-Verschlüsselung geschützt werden.

Informationen zur Aktivierung von HTTPS auf Ihrem Server finden Sie unter Tutorial: Konfiguration SSL/TLS am AL2.

Schritt 2: Testen Ihres Lamp-Servers

Wenn Ihr Server installiert ist und läuft und Ihre Dateiberechtigungen korrekt eingestellt sind, müsste für Ihr `ec2-user`-Konto die Erstellung einer PHP-Datei im Verzeichnis `/var/www/html` möglich sein, auf die über das Internet zugegriffen werden kann.

So testen Sie Ihren LAMP-Server

1. Erstellen Sie eine PHP-Datei im Dokumenten-Stammverzeichnis von Apache.

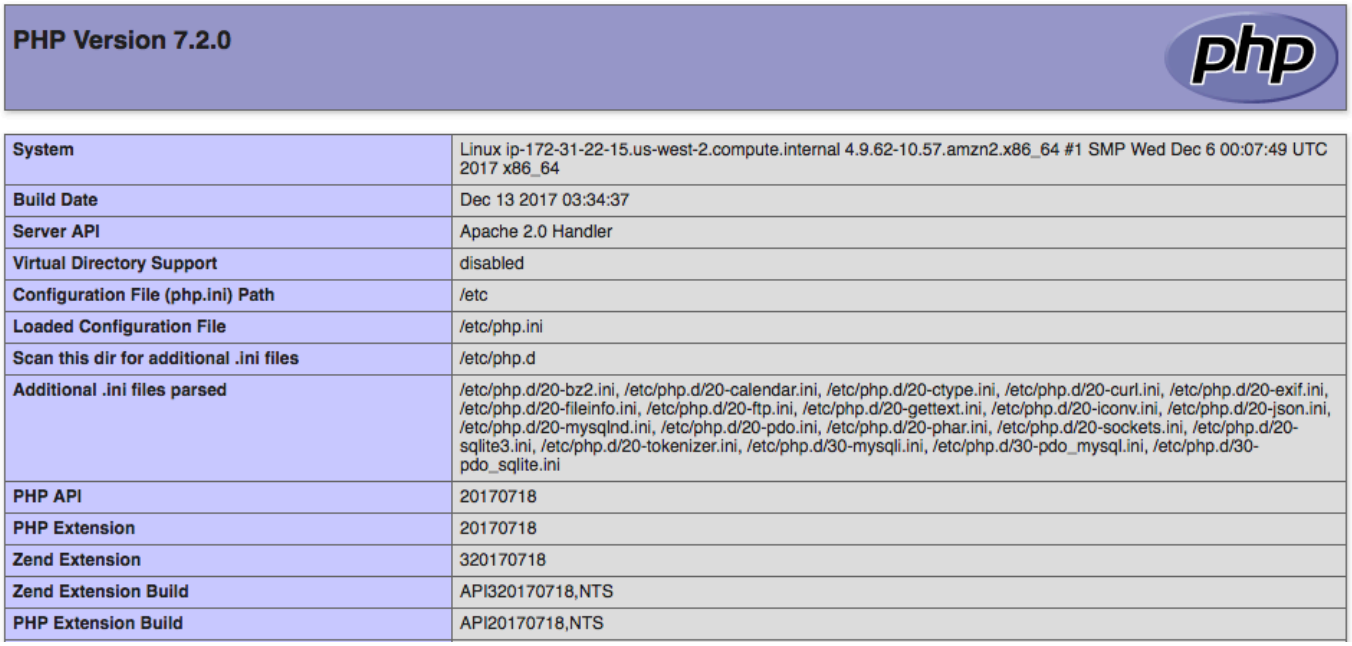
   ```
   [ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
   ```

   Wenn beim Ausführen dieses Befehls der Fehler „Permission denied“ angezeigt wird, melden Sie sich ab und anschließend wieder an, damit die richtigen Gruppenberechtigungen übernommen werden, die Sie in konfiguriert habe So richten Sie Dateiberechtigungen ein.

2. Geben Sie in einem Webbrowser die URL der Datei ein, die Sie gerade erstellt haben. Diese URL ist die öffentliche DNS-Adresse Ihrer Instance, gefolgt von einem Schrägstrich und dem Dateinamen. Beispiel:

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

   Die PHP-Informationsseite wird angezeigt:



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

Wenn diese Seite nicht angezeigt wird, überprüfen Sie, ob die Datei `/var/www/html/phpinfo.php` im vorherigen Schritt ordnungsgemäß angelegt wurde. Mit dem folgenden Befehl können Sie auch überprüfen, ob alle erforderlichen Pakete installiert wurden.

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

Wenn eines der erforderlichen Pakete in Ihrem Ergebnis nicht aufgelistet ist, installieren Sie es mit dem Befehl sudo yum install *package*. Überprüfen Sie außerdem in der Ausgabe des Befehls amazon-linux-extras, ob die `php7.2`- und `lamp-mariadb10.2-php7.2`-Extras aktiviert sind.

3. Löschen Sie die Datei `phpinfo.php`. Obwohl sie nützliche Informationen enthalten könnte, sollte sie aus Sicherheitsgründen nicht über das Internet übertragen werden.

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

Sie sollten nun über einen voll funktionsfähigen LAMP-Webserver verfügen. Wenn Sie zum Dokumenten-Stammverzeichnis von Apache unter `/var/www/html` Inhalte hinzufügen, können Sie diese unter der öffentlichen DNS-Adresse für Ihre Instance anzeigen.

Schritt 3: Sichern des Datenbankservers

Die Standardinstallation des MariaDB-Servers verfügt über mehrere Funktionen, die hervorragend zum Testen und für die Entwicklung geeignet sind, aber bei Produktionsservern sollten Sie deaktiviert oder entfernt werden. Mit dem Befehl mysql_secure_installation rufen Sie eine Anleitung dazu auf, wie Sie ein Stammpasswort einrichten und die unsicheren Funktionen aus Ihrer Installation entfernen. Auch wenn Sie nicht vorhaben, den MariaDB-Server zu verwenden, empfehlen wir Ihnen die Durchführung dieses Verfahrens.

Sichern des MariaDB-Servers

1. Starten Sie den MariaDB-Server.

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

2. Führen Sie mysql_secure_installation.

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

   a. Geben Sie das Passwort für das Stammkonto ein, wenn Sie dazu aufgefordert werden.

      i. Geben Sie das aktuelle Stammpasswort ein. Standardmäßig ist für das Stammkonto kein Passwort eingerichtet. Drücken Sie die Eingabetaste.

      ii. Drücken Sie **Y**, um ein Passwort einzurichten, und geben Sie ein sicheres Passwort zweimal ein. Weitere Hinweise zur Erstellung eines sicheren Passworts finden Sie unter https://identitysafe.norton.com/password-generator/. Bewahren Sie dieses Passwort an einem sicheren Ort auf.

      Die Einrichtung eines Stammpassworts für MariaDB ist nur die grundlegendste Maßnahme, um Ihre Datenbank abzusichern. Wenn Sie eine datenbankgestützte Anwendung aufbauen oder installieren, legen Sie für diese Anwendung normalerweise einen Datenbank-Servicebenutzer an und nutzen das Stammkonto ausschließlich zur Datenbankverwaltung.

   b. Geben Sie **Y** ein, um die anonymen Benutzerkonten zu entfernen.

   c. Geben Sie **Y** ein, um die Root-Anmeldung per Remote-Zugriff zu deaktivieren.

   d. Geben Sie **Y** ein, um die Testdatenbank zu entfernen.

   e. Geben Sie **Y** ein, um die Tabellen mit den Berechtigungen neu zu laden. Speichern Sie anschließend Ihre Änderungen.

3. (Optional) Wenn Sie nicht vorhaben, den MariaDB-Server weiter zu verwenden, stoppen Sie ihn. Sie können ihn erneut starten, wenn Sie ihn wieder brauchen.

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

4. (Optional) Wenn Sie wollen, dass der MariaDB-Server bei jedem Systemstart gestartet wird, geben Sie den folgenden Befehl ein.

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

Schritt 4: (Optional) Installieren phpMyAdmin

phpMyAdminist ein webbasiertes Datenbankverwaltungstool, mit dem Sie die MySQL-Datenbanken auf Ihrer EC2 Instanz anzeigen und bearbeiten können. Führen Sie die unten genannten Schritte durch, um `phpMyAdmin` auf Ihrer Amazon Linux-Instance zu installieren und zu konfigurieren.

> **Important**
>
> Wir empfehlen, es nicht für `phpMyAdmin` den Zugriff auf einen LAMP-Server zu verwenden, es sei denn, Sie haben es SSL/TLS in Apache aktiviert. Andernfalls werden Ihr Datenbankadministratorkennwort und andere Daten unsicher über das Internet übertragen. Sicherheitsempfehlungen der Entwickler finden Sie unter Sichern Ihrer phpMyAdmin Installation. Allgemeine Informationen zum Sichern eines Webservers auf einer EC2 Instance finden Sie unterTutorial: Konfiguration SSL/TLS am AL2.

Um zu installieren phpMyAdmin

1. Installieren Sie die erforderlichen Abhängigkeiten.

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

2. Starten Sie Apache erneut.

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

3. Starten Sie `php-fpm` neu.

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

4. Navigieren Sie zum Stammverzeichnis von Apache unter `/var/www/html`.

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

5. Wählen Sie unter https://www.phpmyadmin.net/downloads ein Quellpaket für die neueste phpMyAdmin Version aus. Um die Datei direkt in Ihre Instance herunterzuladen, kopieren Sie den Link in einen wget-Befehl wie im folgenden Beispiel:

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

6. Erstellen Sie mit dem folgenden Befehl einen `phpMyAdmin`-Ordner und extrahieren Sie das Paket in diesen.

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

7. Löschen Sie den *`phpMyAdmin-latest-all-languages.tar.gz`* Tarball.

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

8. (Optional) Wenn der MySQL-Server nicht ausgeführt wird, starten Sie ihn jetzt.

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

9. Geben Sie in einem Webbrowser die URL Ihrer phpMyAdmin Installation ein. Diese URL ist die öffentliche DNS-Adresse (oder die öffentliche IP-Adresse) Ihrer Instance gefolgt von einem Schrägstrich und dem Namen wie im folgenden Beispiel: Beispiel:

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

Sie sollten die phpMyAdmin Anmeldeseite sehen:

10. Melden Sie sich mit dem `root` Benutzernamen und dem MySQL-Root-Passwort, das Sie zuvor erstellt haben, bei Ihrer phpMyAdmin Installation an.

    Ihre Installation muss vor der Inbetriebnahme noch konfiguriert werden. Wir schlagen vor, dass Sie zunächst die Konfigurationsdatei wie folgt manuell erstellen:

    a. Um mit einer minimalen Konfigurationsdatei zu beginnen, erstellen Sie mit Ihrem bevorzugten Texteditor eine neue Datei und kopieren Sie dann den Inhalt von `config.sample.inc.php` hinein.

    b. Speichern Sie die Datei `config.inc.php` in dem phpMyAdmin Verzeichnis, das enthält`index.php`.

    c. Weitere Einstellungen finden Sie in den Anweisungen nach der Dateierstellung im Abschnitt Verwenden des Setup-Skripts der phpMyAdmin Installationsanweisungen.

Informationen zur Verwendung phpMyAdmin finden Sie im phpMyAdmin Benutzerhandbuch.

Fehlerbehebung

Dieser Abschnitt enthält Vorschläge zum Lösen häufiger Probleme, die bei der Einrichtung eines neuen LAMP-Servers auftreten können.

Ich kann zu meinem Server keine Verbindung über einen Webbrowser herstellen

Führen Sie die folgende Prüfungen durch, um zu sehen, ob Ihr Apache-Webserver ausgeführt wird und auf ihn zugegriffen werden kann.

- Wird der Webserver ausgeführt?

  Mit folgendem Befehl können Sie prüfen, ob der Befehl httpd ausgeführt wird:

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

  Wenn der httpd-Prozess nicht ausgeführt wird, wiederholen Sie die unter Vorbereiten des LAMP-Servers beschriebenen Schritte.
- Ist die Firewall richtig konfiguriert?

  Stellen Sie sicher, dass die Sicherheitsgruppe für die Instance eine Regel enthält, die HTTP-Datenverkehr auf Port 80 zulässt. Weitere Informationen finden Sie unter Regeln zur Sicherheitsgruppe hinzufügen.

Ich kann über HTTPS keine Verbindung zu meinem Server herstellen

Führen Sie die folgende Prüfungen durch, um zu sehen, ob Ihr Apache-Webserver konfiguriert ist, HTTPS zu unterstützen.

- Ist der Webserver richtig konfiguriert?

  Nach der Installation von Apache ist der Server für HTTP-Verkehr konfiguriert. Um HTTPS zu unterstützen, aktivieren Sie TLS auf dem Server und installieren Sie ein SSL-Zertifikat. Weitere Informationen finden Sie unter Tutorial: Konfiguration SSL/TLS am AL2.
- Ist die Firewall richtig konfiguriert?

Stellen Sie sicher, dass die Sicherheitsgruppe für die Instance eine Regel enthält, die HTTPS-Datenverkehr auf Port 443 zulässt. Weitere Informationen finden Sie unter Regeln zu einer Sicherheitsgruppe hinzufügen.

Verwandte Themen

Weitere Informationen zum Übertragen von Dateien auf Ihre Instance oder zum Installieren eines WordPress Blogs auf Ihrem Webserver finden Sie in der folgenden Dokumentation:

- Übertragen Sie Dateien auf Ihre Linux-Instance mit WinSCP.
- Übertragen Sie Dateien mithilfe eines SCP Clients auf Linux-Instances.
- Tutorial: Hosten Sie einen WordPress Blog auf AL2

Weitere Informationen über die in diesem Tutorial verwendete(n) Befehle und Software finden Sie auf den folgenden Webseiten:

- Apache-Webserver: http://httpd.apache.org/
- MariaDB-Datenbankserver: https://mariadb.org/
- PHP-Programmiersprache: http://php.net/
- Der `chmod` Befehl: https://en.wikipedia. org/wiki/Chmod
- Der `chown` Befehl: https://en.wikipedia. org/wiki/Chown

Weitere Informationen zum Registrieren eines Domain-Namens für Ihren Webserver oder zum Übertragen eines bestehenden Domain-Namens auf diesen Host finden Sie unter Erstellen und Migrieren von Domains und Sub-Domains zu Amazon Route 53 im Entwicklerhandbuch für Amazon Route 53.

Tutorial: Konfiguration SSL/TLS am 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/TLSauf einer EC2 Instanz mit AL2 einem Apache-Webserver). In diesem Tutorial wird davon ausgegangen, dass Sie keinen Load Balancer verwenden. Wenn Sie Elastic Load Balancing verwenden, können Sie im Load Balancer SSL-Offload konfigurieren und stattdessen ein Zertifikat aus AWS Certificate Manager verwenden.

Aus historischen Gründen wird die Webverschlüsselung häufig einfach als SSL bezeichnet. Auch wenn Webbrowser SSL weiterhin unterstützen, ist das Nachfolgeprotokoll TLS weniger anfällig für Angriffe. AL2 deaktiviert standardmäßig die serverseitige Unterstützung für alle Versionen von SSL. Gremien für Sicherheitsstandards erachten TLS 1.0 als unsicher. TLS 1.0 und TLS 1.1 wurden im März 2021 formell veraltet. Dieses Tutorial enthält Empfehlungen, die ausschließlich auf der Aktivierung von TLS 1.2 basieren. TLS 1.3 wurde 2018 fertiggestellt und ist verfügbar, AL2 solange die zugrunde liegende TLS-Bibliothek (OpenSSL in diesem Tutorial) unterstützt und aktiviert ist. Kunden müssen spätestens zum 28. Juni 2023 TLS 1.2 oder höher unterstützen. Weitere Informationen zum aktualisierten Verschlüsselungsstandard finden Sie unter RFC 7568 und RFC 8446.

Dieses Tutorial bezieht sich auf TLS als moderne Web-Verschlüsselung.

Important

Diese Verfahren sind für die Verwendung mit vorgesehen. AL2 Wir gehen auch davon aus, dass Sie mit einer neuen EC2 Amazon-Instance beginnen. Wenn Sie versuchen, eine EC2 Instance einzurichten, auf der eine andere Distribution ausgeführt wird, oder eine Instance, auf der eine alte Version von ausgeführt wird AL2, funktionieren einige Verfahren in diesem Tutorial möglicherweise nicht. Für Ubuntu lesen Sie bitte die folgende Community-Dokumentation: Open SSL auf Ubuntu. Informationen zu Red Hat Enterprise Linux finden Sie im Thema Apache-HTTP-Webserver einrichten. Andere Verteilungen finden Sie in der jeweiligen Dokumentation.

Note

Alternativ können Sie AWS Certificate Manager (ACM) für AWS Nitro-Enklaven verwenden. Dabei handelt es sich um eine Enklave-Anwendung, mit der Sie öffentliche und private SSL/TLS Zertifikate für Ihre Webanwendungen und Server verwenden können, die auf EC2 Amazon-Instances mit Nitro Enclaves ausgeführt werden. AWS Nitro Enclaves ist eine EC2 Amazon-Funktion, die die Schaffung isolierter Computerumgebungen ermöglicht, um hochsensible Daten wie SSL/TLS Zertifikate und private Schlüssel zu schützen und sicher zu verarbeiten.
ACM for Nitro Enclaves arbeitet mit Nginx, das auf Ihrer Amazon EC2 Linux-Instance ausgeführt wird, um private Schlüssel zu erstellen, Zertifikate und private Schlüssel zu verteilen und Zertifikatserneuerungen zu verwalten.

Um ACM for Nitro Enclaves verwenden zu können, müssen Sie eine Enclave-fähige Linux-Instance nutzen.
Weitere Informationen finden Sie unter Was ist Nitro Enclaves? AWS und AWS Certificate Manager für Nitro Enclaves im Nitro Enclaves-Benutzerhandbuch.AWS

Inhalt

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, führen Sie die folgenden Schritte aus:

- Starten Sie eine Amazon EBS-gestützte AL2 Instance. Weitere Informationen finden Sie unter Launch an Instance im EC2 Amazon-Benutzerhandbuch.
- Konfigurieren Sie Ihre Sicherheitsgruppen so, dass Ihre Instance Verbindungen auf den folgenden TCP-Ports akzeptieren kann:
  - SSH (Port 22)
  - HTTP (Port 80)
  - HTTPS (Port 443)

  Weitere Informationen finden Sie unter Regeln für Sicherheitsgruppen im EC2 Amazon-Benutzerhandbuch.
- Installieren Sie den Apache-Webserver. step-by-stepAnweisungen finden Sie unter Tutorial: Installieren Sie einen LAMP-Webserver auf AL2. Es werden nur das httpd-Paket und die zugehörigen Abhängigkeiten benötigt, sodass die Anleitungen mit PHP und MariaDB ignoriert werden können.
- Zum Identifizieren und Authentifizieren von Websites verwendet die Public Key-Infrastruktur (PKI) TLS das Domain Name System (DNS). Um Ihre EC2 Instance zum Hosten einer öffentlichen Website zu verwenden, müssen Sie einen Domainnamen für Ihren Webserver registrieren oder einen vorhandenen Domainnamen auf Ihren EC2 Amazon-Host übertragen. Dafür sind zahlreiche

Drittanbieterservices für die Domain-Registrierung und das DNS-Hosting verfügbar. Oder Sie verwenden Amazon Route 53.

Schritt 1: Aktivieren von TLS auf dem Server

Option: Abschließen dieses Tutorials mit Automation

Um dieses Tutorial mithilfe von AWS Systems Manager Automatisierung anstelle der folgenden Aufgaben abzuschließen, führen Sie das Automatisierungsdokument aus.

Dieses Verfahren führt Sie durch den Prozess der Einrichtung von TLS AL2 mit einem selbstsignierten digitalen Zertifikat.

> **Note**
>
> Ein selbstsigniertes Zertifikat kann zu Testzwecken, jedoch nicht für die Produktion verwendet werden. Wenn Sie Ihr selbstsigniertes Zertifikat im Internet bereitstellen, werden den Besuchern Ihrer Website Sicherheitswarnungen angezeigt.

So aktivieren Sie TLS auf einem Server

1. Verbinden Sie sich mit der Instance und stellen Sie sicher, dass Apache ausgeführt wird.

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

   Wenn der zurückgegebene Wert nicht „enabled“ (aktiviert) ist, starten Sie Apache und richten es so ein, dass es bei jedem Neustart des Systems gestartet wird.

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

2. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus. Dieser Vorgang kann einige Minuten dauern. Es ist jedoch wichtig, sicherzustellen, dass Sie über die aktuellen Sicherheitsaktualisierungen und Fehlerbehebungen verfügen.

> **Note**
>
> Mit der Option `-y` werden die Updates installiert, ohne um Bestätigung zu bitten. Wenn Sie die Aktualisierungen vor der Installation überprüfen möchten, können Sie diese Option auslassen.

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

3. Wenn Ihre Instance jetzt aktuell ist, fügen Sie TLS-Unterstützung hinzu, indem Sie das Apache-Modul installiere `mod_ssl`.

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

Ihre Instance verfügt nun über die folgenden Dateien, mit denen Sie Ihren sicheren Server konfigurieren und ein Zertifikat zum Testen erstellen:

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

  Die Konfigurationsdatei für mod_ssl. Diese enthält Richtlinien, die Apache mitteilen, wo Verschlüsselungsschlüssel und Zertifikate, die zu genehmigenden TLS-Protokollversionen und die zu akzeptierenden Verschlüsselungschiffren gefunden werden können.

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

  Ein Skript zum Generieren eines selbstsignierten X.509-Zertifikats und privaten Schlüssels für Ihren Server-Host. Dieses Zertifikat ist nützlich zum Testen, ob Apache ordnungsgemäß für die Verwendung von TLS eingerichtet ist. Da es keinen Identitätsnachweis liefert, sollte es in der Produktion nicht verwendet werden. Wenn es in der Produktion eingesetzt wird, löst es Warnungen in Web-Browsern aus.

4. Führen Sie das Skript aus, um ein selbstsigniertes Dummy-Zertifikat und einen Schlüssel für die Überprüfung zu generieren.

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

Dadurch wird eine neue Datei `localhost.crt` im Verzeichnis `/etc/pki/tls/certs/` erstellt. Der angegebene Dateiname entspricht dem Standard, der in der SSLCertificateFile-Direktive in `/etc/httpd/conf.d/ssl.conf` zugewiesen ist.

Die Datei enthält sowohl ein selbstsigniertes Zertifikat als auch den privaten Schlüssel des Zertifikats. Für Apache müssen das Zertifikat und der Schlüssel im PEM-Format sein. Diese bestehen aus Base64-kodierten ASCII-Zeichen, die durch „BEGIN” und „END”-Zeilen eingerahmt werden, wie im folgendem, verkürzten Beispiel dargestellt.

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

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

Die Dateinamen und Erweiterungen dienen der Einfachheit und haben keinerlei Auswirkungen auf die Funktion. Sie können beispielsweise ein Zertifikat mit `cert.crt`, `cert.pem` oder einem beliebigen anderen Dateinamen benennen, solange die zugehörige Richtlinie in der Datei `ssl.conf` denselben Namen verwendet.

> **Note**
>
> Wenn Sie die TLS-Standarddateien mit Ihren eigenen benutzerdefinierten Dateien ersetzen, müssen diese das PEM-Format aufweisen.

5. Öffnen Sie die `/etc/httpd/conf.d/ssl.conf`-Datei mit ihrem bevorzugten Texteditor (z. B. vim oder nano) als Root-Benutzer und kommentieren Sie die folgende Zeile aus, da das selbstsignierte Dummy-Zertifikat auch den Schlüssel enthält. Wenn Sie diese Zeile nicht auskommentieren, bevor Sie den nächsten Schritt abschließen, kann der Apache-Service nicht gestartet werden.

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

6. Starten Sie Apache erneut.

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

   > **Note**
   >
   > Stellen Sie sicher, dass der TCP-Port 443 auf Ihrer EC2 Instance zugänglich ist, wie zuvor beschrieben.

7. Ihr Apache-Webserver sollte jetzt HTTPS (sicheres HTTP) über Port 443 unterstützen. Testen Sie es, indem Sie die IP-Adresse oder den vollqualifizierten Domainnamen Ihrer EC2 Instanz in eine Browser-URL-Leiste mit dem Präfix eingeben**`https://`**.

   Da Sie eine Verbindung mit einer Website mit einem selbstsignierten, nicht vertrauenswürdigen Host-Zertifikat herstellen, zeigt Ihr Browser möglicherweise eine Reihe von Sicherheitswarnungen an. Setzen Sie die Warnmeldungen außer Kraft und fahren Sie mit der Website fort.

   Wenn die Apache-Standardtestseite geöffnet wird, bedeutet dies, dass Sie TLS erfolgreich auf Ihrem Server konfiguriert haben. Alle Daten, die zwischen dem Browser und dem Server übertragen werden, sind nun verschlüsselt.

> **Note**
>
> Damit den Besuchern keine Warnbildschirme angezeigt werden, müssen Sie ein vertrauenswürdiges, CA-signiertes Zertifikat abrufen, das nicht nur verschlüsselt, sondern Sie auch öffentlich als den Besitzer der Website authentifiziert.

Schritt 2: Abrufen eines CA-signierten Zertifikats

Sie können das folgende Verfahren verwenden, um ein CA-signiertes Zertifikat zu erhalten:

- Erzeugen Sie aus dem privaten Schlüssel eine Zertifikatssignierungsanforderung (Certificate Signing Request, CSR)
- Senden Sie die CSR an eine Zertifizierungsstelle (CA)
- Sie erhalten ein signiertes Host-Zertifikat
- Konfigurieren Sie Apache, um das Zertifikat zu verwenden

Ein selbstsigniertes TLS-X.509-Host-Zertifikat ist kryptologisch mit einem CA-signierten Zertifikat identisch. Der Unterschied liegt im sozialen, nicht im mathematischen Bereich. Eine CA validiert zumindest den Besitzer einer Domain, bevor ein Zertifikat für einen Antragsteller ausgegeben wird. Jeder Webbrowser enthält eine Liste der vom Browserhersteller zu diesem Zweck CAs vertrauenswürdigen Websites. Ein X.509-Zertifikat besteht hauptsächlich aus einem öffentlichen Schlüssel, der Ihrem privaten Serverschlüssel entspricht, sowie einer Signatur durch die CA, die kryptografisch an den öffentlichen Schlüssel gebunden ist. Wenn ein Browser über HTTPS eine Verbindung zu einem Webserver herstellt, präsentiert der Server dem Browser ein Zertifikat, das er anhand seiner Liste vertrauenswürdiger Server überprüfen kann CAs. Wenn sich der Aussteller auf der Liste befindet oder über eine Vertrauenskette aus anderen vertrauenswürdigen Ausstellern zugänglich ist, handelt der Browser einen schnellen verschlüsselten Datenkanal mit dem Server aus und lädt die Seite.

Im Allgemeinen sind Zertifikate aufgrund der Arbeit im Zusammenhang mit der Validierung der Anforderungen kostenpflichtig, deshalb lohnt es sich, die Angebote zu vergleichen. Einige CAs bieten kostenlose Basiszertifikate an. Das bemerkenswerteste davon CAs ist das Let's Encrypt-Projekt, das auch die Automatisierung des Prozesses zur Erstellung und Verlängerung von Zertifikaten unterstützt. Weitere Informationen zur Verwendung eines Let's Encrypt-Zertifikats finden Sie unter Get Certbot.

Wenn Sie beabsichtigen, kommerzielle Dienstleistungen anzubieten, ist AWS Certificate Manager eine gute Option.

Dem Host-Zertifikat liegt der Schlüssel zugrunde. Seit 2019 empfehlen Regierungs- und Branchengruppen eine Schlüssel(-Modul)-Mindestgröße von 2048 Bits für RSA-Schlüssel, die Dokumente bis 2030 schützen sollen. Die von OpenSSL generierte Standardmodulgröße AL2 beträgt 2048 Bit, was für die Verwendung in einem CA-signierten Zertifikat geeignet ist. Im folgenden Verfahren ist ein optionaler Schritt für diejenigen vorgesehen, die einen benutzerdefinierten Schlüssel verwenden möchten, z.B. einen mit einem größeren Modul oder mit einem anderen Verschlüsselungsalgorithmus.

> **Important**
>
> Diese Anweisungen zum Erwerb eines CA-signierten Host-Zertifikats funktioniert nur, wenn Sie eine registrierte und gehostete DNS-Domain besitzen.

So rufen Sie ein CA-signierten Zertifikat ab

1. Connect zu Ihrer Instance her und navigieren Sie zu/etc/pki/tls/private/. Dies ist das Verzeichnis, in dem Sie den privaten Schlüssel des Servers für TLS speichern. Wenn Sie lieber Ihren vorhandenen Host-Schlüssel zum Generieren der CSR verwenden möchten, fahren Sie mit Schritt 3 fort.
2. (Optional) Generieren Sie einen neuen privaten Schlüssel. Hier sind einige Beispiele für Schlüsselkonfigurationen. Jeder der resultierenden Schlüssel funktioniert mit Ihrem Webserver, aber sie unterscheiden sich durch den Grad und die Art der Sicherheit, die sie implementieren.
   - Beispiel 1: Erstellen Sie einen Standard-RSA-Hostschlüssel. Bei der erstellten Datei, **`custom.key`**, handelt es sich um einen privaten 2048-Bit-RSA-Schlüssel.

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

   - Beispiel 2: Erstellen Sie einen stärkeren RSA-Schlüssel mit einem größeren Modul. Bei der erstellten Datei, **`custom.key`**, handelt es sich um einen privaten 4096-Bit-RSA-Schlüssel.

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

- Beispiel 3: Erstellen Sie einen 4096-Bit-verschlüsselten RSA-Schlüssel mit Passwortschutz. Die resultierende Datei, **`custom.key`**, ist ein privater 4096-Bit-RSA-Schlüssel, der mit der AES-128-Verschlüsselung verschlüsselt ist.

  > **Important**
  >
  > Die Verschlüsselung des Schlüssels bietet höhere Sicherheit. Da für einen verschlüsselten Schlüssel ein Passwort erforderlich ist, können von diesem abhängige Services jedoch nicht automatisch gestartet werden. Jedes Mal, wenn Sie diesen Schlüssel verwenden, müssen Sie das Passwort (im vorhergehenden Beispiel „abcde12345“) über eine SSH-Verbindung bereitstellen.

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

- Beispiel 4: Erstellen Sie einen Schlüssel mit einer Nicht-RSA-Verschlüsselung. Die RSA-Kryptografie kann aufgrund der Größe ihrer öffentlichen Schlüssel, die auf dem Produkt aus zwei großen Primzahlen basieren, relativ langsam sein. Es ist jedoch möglich, Schlüssel für TLS zu erstellen, die andere Verschlüsselungschiffren als RSA verwenden. Schlüssel, die auf der Mathematik von Ellipsenkurven basieren, sind kleiner und bieten eine schnellere Rechenleistung bei der Bereitstellung einer gleichwertigen Sicherheitsebene.

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

  Das Ergebnis ist ein privater Ellipsenkurvenschlüssel mit 256-Bit, der prime256v1 verwendet, einer „benannten Kurve“, die OpenSSL unterstützt. Die kryptografische Stärke ist hierbei laut NIST etwas höher als bei einem 2048-Bit-RSA-Schlüssel.

  > **Note**
  >
  > Nicht alle CAs bieten dieselbe Unterstützung für elliptic-curve-based Schlüssel wie für RSA-Schlüssel.

Stellen Sie sicher, dass der neue private Schlüssel sehr restriktive Besitzrechte und Berechtigungen hat (owner = root, group=root, read/write nur für Besitzer). Führen Sie die Befehle wie im folgenden Beispiel veranschaulicht aus.

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

Die vorhergehenden Befehle erzeugen das folgende Ergebnis.

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

Wenn Sie einen zufriedenstellenden Schlüssel erstellt und konfiguriert haben, können Sie eine CSR erstellen.

3. Erstellen Sie eine CSR mit Ihrem bevorzugten Schlüssel. Im folgenden Beispiel wird verwende **`custom.key`**.

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

OpenSSL öffnet einen Dialog und fordert Sie auf, die in der folgenden Tabelle aufgeführten Informationen einzugeben. Alle Felder außer Common Name (Allgemeiner Name) sind bei einem grundlegenden, Domain-validierten Host-Zertifikat optional.

Name	Beschreibung	Beispiel
Ländername	Die zweistellige ISO-Abkürzung für Ihr Land	US (=United States, Vereinigte Staaten)
State or Province Name	Der Name des Bundesstaats oder der Provinz, in dem bzw. der sich Ihre Organisation befindet. Dieser Name darf nicht abgekürzt werden.	Washington
Locality Name	Der Standort Ihrer Organisation, wie beispielsweise eine Stadt.	Seattle

Name	Beschreibung	Beispiel
Name der Organisation	Der vollständige, offizielle Name Ihrer Organisation. Kürzen Sie den Namen Ihrer Organisation nicht ab.	Beispielunternehmen
Organizational Unit Name	Zusätzliche Informationen zu Ihrer Organisation, sofern vorhanden.	Beispielabteilung
Common Name	Dieser Wert muss genau der Webadresse entsprechen, die Ihre Benutzer in einen Browser eingeben sollen. Dies ist in der Regel ein Domain-Name mit einem vorangestellten Hostnamen oder Alias in der Form **`www.example.com`** . Beim Testen mit einem selbstsignierten Zertifikat und ohne DNS-Auflösung kann der allgemeine Name nur aus dem Hostnamen bestehen. CAs bieten auch teurere Zertifikate an, die Platzhalternamen akzeptieren, wie z. **`*.example.com`**	www.example.com
Email Address	Die E-Mail-Adresse des Serveradministrators.	someone@example.com

Zuletzt fordert OpenSSL Sie zur Eingabe eines optionalen Challenge-Passworts auf. Dieses Passwort gilt nur für die CSR und für Transaktionen zwischen Ihnen und Ihrer CA. Befolgen Sie daher die Empfehlungen Ihrer CA diesbezüglich und in Bezug auf das andere optionale Feld, den optionalen Unternehmensnamen. Das CSR-Challenge-Passwort wirkt sich nicht auf den Serverbetrieb aus.

Die erstellte Datei **`csr.pem`** enthält Ihren öffentlichen Schlüssel, die digitale Signatur Ihres öffentlichen Schlüssels und die von Ihnen eingegebenen Metadaten.

4. Übermitteln Sie die CSR an eine CA. Dies besteht in der Regel daraus, Ihre CSR-Datei in einem Texteditor zu öffnen und den Inhalt in ein Webformular zu kopieren. Zu diesem Zeitpunkt werden Sie möglicherweise aufgefordert, einen oder mehrere alternative Namen (SANs) für das Zertifikat

anzugeben. Wenn **`www.example.com`** der allgemeine Name ist, wäre **`example.com`** ein guter SAN und umgekehrt. Ein Besucher Ihrer Website, der einen dieser Namen eingibt, wird eine fehlerfreie Verbindung sehen. Wenn Ihr CA-Webformular dies zulässt, nehmen Sie den allgemeinen Namen in die Liste der auf SANs. Manche CAs schließen ihn automatisch ein.

Nachdem Ihre Anfrage genehmigt wurde, erhalten Sie ein neues, von der CA unterzeichnetes Host-Zertifikat. Möglicherweise werden Sie auch dazu aufgefordert, eine Zwischenzertifikatsdatei herunterzuladen, die zusätzliche Zertifikate enthält, welche zum Fertigstellen der Vertrauenskette der CA benötigt werden.

> **Note**
>
> Ihre CA kann Ihnen Dateien in verschiedenen Formaten für verschiedene Zwecke zusenden. Für dieses Tutorial sollten Sie nur eine Zertifikatsdatei im PEM-Format verwenden, die in der Regel (aber nicht immer) mit der Dateierweiterung `.pem` oder `.crt` gekennzeichnet ist. Wenn Sie sich nicht sicher sind, welche Datei Sie verwenden sollen, öffnen Sie die Dateien mit einem Texteditor und suchen Sie die Datei, die einen oder mehrere Blöcke enthält, die mit der folgenden Zeile beginnen.
>
> ```
> - - - - -BEGIN CERTIFICATE - - - - -
> ```
>
> Die Datei sollte darüber hinaus mit der folgenden Zeile enden.
>
> ```
> - - - -END CERTIFICATE - - - - -
> ```
>
> Sie können die Datei auch in der Befehlszeile testen, wie im Folgenden gezeigt.
>
> ```
> [ec2-user certs]$ openssl x509 -in certificate.crt -text
> ```
>
> Vergewissern Sie sich, dass diese Zeilen in der Datei erscheinen. Verwenden Sie keine Dateien, die mit `.p7b`, `.p7c` oder ähnlichen Dateiendungen enden.

5. Platzieren Sie ein neues CA-signiertes Zertifikat und alle Zwischenzertifikate im `/etc/pki/tls/certs`-Verzeichnis.

> **Note**
>
> Es gibt mehrere Möglichkeiten, Ihr neues Zertifikat auf Ihre EC2 Instanz hochzuladen. Die einfachste und informativste Methode besteht jedoch darin, einen Texteditor (z. B. vi, nano oder Notepad) sowohl auf Ihrem lokalen Computer als auch auf Ihrer Instanz zu öffnen und dann den Dateiinhalt zwischen den Instanzen zu kopieren und einzufügen. Sie benötigen Root-Rechte [sudo], um diese Operationen auf der EC2 Instanz auszuführen. Auf diese Weise können Sie sofort erkennen, ob es Probleme mit Berechtigungen oder mit dem Pfad gibt. Achten Sie jedoch darauf, beim Kopieren der Inhalte keine zusätzlichen Zeilen einzufügen und die Inhalte nicht zu ändern.

Überprüfen Sie innerhalb des `/etc/pki/tls/certs` Verzeichnisses, ob die Einstellungen für Dateibesitz, Gruppen und Berechtigungen den stark restriktiven AL2 Standardeinstellungen entsprechen (owner=root, group=root, nur für Besitzer). read/write Das folgende Beispiel zeigt die zu verwendenden Befehle.

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

Diese Befehle sollten das folgende Ergebnis hervorrufen.

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

Die Berechtigungen für die Zwischenzertifikatsdatei sind weniger strikt (Eigentümer=root, Gruppe=root, Eigentümer kann schreiben, Gruppe kann lesen, die restliche Welt kann lesen). Das folgende Beispiel zeigt die zu verwendenden Befehle.

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

Diese Befehle sollten das folgende Ergebnis hervorrufen.

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

6. Legen Sie den privaten Schlüssel, den Sie zum Erstellen der CSR verwendet haben, in das Verzeichnis `/etc/pki/tls/private/`.

   > **Note**
   >
   > Es gibt mehrere Möglichkeiten, Ihren benutzerdefinierten Schlüssel auf Ihre EC2 Instanz hochzuladen. Die einfachste und informativste Methode besteht jedoch darin, einen Texteditor (z. B. vi, nano oder Notepad) sowohl auf Ihrem lokalen Computer als auch auf Ihrer Instanz zu öffnen und dann den Dateiinhalt zwischen ihnen zu kopieren und einzufügen. Sie benötigen Root-Rechte [sudo], wenn Sie diese Operationen auf der EC2 Instanz ausführen möchten. Auf diese Weise können Sie sofort erkennen, ob es Probleme mit Berechtigungen oder mit dem Pfad gibt. Achten Sie jedoch darauf, beim Kopieren der Inhalte keine zusätzlichen Zeilen einzufügen und die Inhalte nicht zu ändern.

   Verwenden Sie innerhalb des `/etc/pki/tls/private` Verzeichnisses die folgenden Befehle, um zu überprüfen, ob die Einstellungen für Dateibesitz, Gruppen und Berechtigungen den stark restriktiven AL2 Standardeinstellungen entsprechen (owner=root, group=root, nur für Besitzer). 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
   ```

   Diese Befehle sollten das folgende Ergebnis hervorrufen.

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

7. Bearbeiten Sie die Datei `/etc/httpd/conf.d/ssl.conf` so, dass sie Ihr neues Zertifikat und Ihre Schlüsseldateien widerspiegelt.

   a. Geben Sie den Pfad und Dateinamen des CA-signierten Host-Zertifikats im `SSLCertificateFile`-Verzeichnis von Apache an.

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

b. Wenn Sie eine Zwischenzertifikatsdatei erhalten haben (`intermediate.crt` in diesem Beispiel), stellen Sie den entsprechenden Pfad und Dateinamen über das `SSLCACertificateFile`-Verzeichnis in Apache bereit:

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

> **Note**
>
> Manche CAs kombinieren das Host-Zertifikat und die Zwischenzertifikate in einer einzigen Datei, sodass die Direktive überflüssig wird. `SSLCACertificateFile` Informieren Sie sich in den von Ihrer CA bereitgestellten Anweisungen.

c. Geben Sie den Pfad und Dateinamen des privaten Schlüssels (in diesem Beispiel `custom.key`) in der `SSLCertificateKeyFile`-Direktive von Apache an:

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

8. Speichern Sie `/etc/httpd/conf.d/ssl.conf` und starten Sie Apache erneut.

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

9. Testen Sie Ihren Server, indem Sie Ihren Domain-Namen in eine Browser-URL-Leiste mit dem Präfix `https://` eingeben. Ihr Browser sollte die Testseite über HTTPS laden, ohne Fehler zu erzeugen.

Schritt 3: Testen und Verstärken der Sicherheitskonfiguration

Wenn Ihre TLS betriebsbereit und öffentlich zugänglich ist, sollten Sie testen, wie sicher sie wirklich ist. Dies ist ganz einfach möglich mithilfe von Online-Services wie beispielsweise Qualys SSL Labs, der eine kostenlose und gründliche Analyse Ihrer Sicherheitseinrichtung durchführt. Basierend auf den Ergebnissen entscheiden Sie sich möglicherweise dafür, die Standard-Sicherheitskonfiguration zu verstärken, indem Sie kontrollieren, welche Protokolle akzeptiert werden sollen, welche Chiffren Sie bevorzugen und welche ausgeschlossen werden soll. Um weitere Informationen zu erhalten, sehen Sie sich an, wie Qualys seine Skalen gestaltet.

> **Important**
>
> Reale Tests sind außerordentlich wichtig für die Sicherheit Ihres Servers. Kleine Konfigurationsfehler führen möglicherweise zu ernsten Sicherheitsverstößen und Datenverlusten. Da sich die empfohlenen Sicherheitsmaßnahmen aufgrund von Forschungen und neuartigen Bedrohungen ständig ändern, sind regelmäßige Sicherheitsprüfungen wichtig für eine gute Serveradministration.

Geben Sie auf der Website von Qualys SSL Labs den vollständigen Domain-Namen Ihres Servers ein, in der Form **`www.example.com`**. Nach ungefähr zwei Minuten erhalten Sie eine Note (von A bis F) für Ihre Website sowie eine detaillierte Auflistung der Ergebnisse. In der folgenden Tabelle wird der Bericht für eine Domain zusammengefasst, deren Einstellungen mit der Standard-Apache-Konfiguration identisch sind AL2, und für die ein Certbot-Standardzertifikat vorhanden ist.

Gesamtbewertung	B
Zertifikat	100 %
Protokollunterstützung	95 %
Schlüsselaustausch	70 %
Chiffrestärke	90 %

Obwohl die Übersicht zeigt, dass die Konfiguration größtenteils intakt ist, zeigt der detaillierte Bericht einige potenzielle Probleme, die hier nach Schweregrad geordnet aufgelistet werden:

✗ Die RC4 Chiffre wird für die Verwendung durch bestimmte ältere Browser unterstützt. Eine Chiffre ist der mathematische Kern eines Verschlüsselungsalgorithmus. RC4, eine schnelle Chiffre, die zur Verschlüsselung von TLS-Datenströmen verwendet wird, weist bekanntermaßen mehrere schwerwiegende Schwächen auf. Wenn Sie nicht sehr gute Gründe haben, veraltete Browser zu unterstützen, sollten Sie dies deaktivieren.

✗ Alte TLS-Versionen werden unterstützt. Die Konfiguration unterstützt TLS 1.0 (bereits veraltet) und TLS 1.1 (demnächst veraltet). Seit 2018 wurde nur TLS 1.2 empfohlen.

✗ Forward Secrecy wird nicht vollständig unterstützt. Forward Secrecy ist ein Feature von Algorithmen zur Verschlüsselung mit temporären (flüchtigen) Sitzungsschlüsseln, die von dem privaten Schlüssel abgeleitet werden. In der Praxis bedeutet dies, dass Angreifen HTTPS-Daten nicht entschlüsseln können, selbst wenn sie den langfristigen privaten Schlüssel eines Webservers besitzen.

So korrigieren Sie die TLS-Konfiguration und machen Sie zukunftssicher

1. Öffnen Sie die Konfigurationsdatei `/etc/httpd/conf.d/ssl.conf` in einem Texteditor und kommentieren Sie die folgende Zeile aus, indem Sie „#“ am Anfang der Zeile eingeben.

   ```
   #SSLProtocol all -SSLv3
   ```

2. Fügen Sie die folgende Richtlinie hinzu:

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

   Diese Richtlinie deaktiviert die SSL-Versionen 2 und 3 explizit sowie auch die TLS-Versionen 1.0 und 1.1. Der Server akzeptiert jetzt keine verschlüsselten Verbindungen mit Clients, die eine andere Version als TLS 1.2 verwenden. Der Verbose-Wortlaut in der Richtlinie teilt einem menschlichen Leser genauer mit, wofür der Server konfiguriert ist.

   > **Note**
   >
   > Durch eine solche Deaktivierung der TLS-Versionen 1.0 und 1.1 wird ein kleiner Prozentsatz von veralteten Webbrowsern daran gehindert, auf Ihre Website zuzugreifen.

So ändern Sie die Liste der zulässigen Chiffren

1. Suchen Sie in der Konfigurationsdatei `/etc/httpd/conf.d/ssl.conf` den Abschnitt mit der **`SSLCipherSuite`**-Richtlinie und kommentieren Sie die bestehende Zeile aus, indem Sie „#“ am Anfang der Zeile eingeben.

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

2. Geben Sie explizite Verschlüsselungssammlungen und eine Verschlüsselungsreihenfolge an, die Forward Secrecy unterstützt und unsichere Verschlüsselungen vermeidet. Die hier

verwendete Richtlinie `SSLCipherSuite` basiert auf der Ausgabe aus dem Mozilla SSL-Konfigurationsgenerator, der eine TLS-Konfiguration an die spezifische Software, die auf Ihrem Server ausgeführt wird, angepasst wird. Bestimmen Sie zunächst Ihre Apache- und OpenSSL-Versionen, indem Sie die Ausgabe der folgenden Befehle verwenden.

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

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

Wenn die zurückgegebenen Informationen beispielsweise Apache 2.4.34 und OpenSSL 1.0.2 sind, geben wir diese in den Generator ein. Wenn Sie das „moderne“ Kompatibilitätsmodell auswählen, wird dadurch eine `SSLCipherSuite`-Richtlinie erstellt, die die Sicherheit aggressiv durchsetzt, aber dennoch für die meisten Browser funktioniert. Wenn die Modemkonfiguration von der Software nicht unterstützt wird, können Sie Ihre Software aktualisieren oder stattdessen die „fortgeschrittene“ Konfiguration wählen.

```
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
```

Die ausgewählten Chiffren weisen ECDHE im Namen auf, eine Abkürzung für Elliptic Curve Diffie-Hellman Ephemeral. Der Begriff Ephemeralität (Flüchtigkeit) gibt die "Forward Secrecy (Folgenlosigkeit)" an. Als Nebenprodukt werden diese Chiffren nicht unterstützt. RC4

Wir empfehlen, eine explizite Liste von Chiffren zu verwenden, anstatt sich auf Standardeinstellungen oder knappe Richtlinien zu verlassen, deren Inhalt nicht sichtbar ist.

Kopieren Sie die erzeugte Richtlinie in `/etc/httpd/conf.d/ssl.conf`.

> **Note**
>
> Obwohl dies hier zur besseren Lesbarkeit auf mehrere Zeilen verteilt ist, muss die Richtlinie in einer einzelnen Zeile mit nur einem Doppelpunkt (ohne Leerstellen) aufgeführt werden, wenn sie nach `/etc/httpd/conf.d/ssl.conf` kopiert wird.

3. Entfernen Sie schließlich die Kommentarzeichen in der folgende Zeile, indem Sie das „#“ am Anfang der Zeile löschen.

   ```
   #SSLHonorCipherOrder on
   ```

   Diese Richtlinie zwingt den Server, hochrangige Chiffren zu bevorzugen, einschließlich derjenigen (in diesem Fall), die Forward Secrecy unterstützen. Wenn diese Richtlinie aktiviert ist, versucht der Server, eine hochgradig sichere Verbindung herzustellen, bevor er auf Chiffren mit geringerer Sicherheit zurückgreift.

Nach Abschluss dieser beiden Verfahren speichern Sie die Änderungen in `/etc/httpd/conf.d/ssl.conf` und starten Sie Apache neu.

Wenn Sie die Domain erneut auf Qualys SSL Labs testen, sollten Sie feststellen, dass die RC4 Sicherheitslücke und andere Warnungen behoben sind und die Zusammenfassung etwa wie folgt aussieht.

Gesamtbewertung	A
Zertifikat	100 %
Protokollunterstützung	100 %
Schlüsselaustausch	90 %
Chiffrestärke	90 %

Mit jeder Aktualisierung von OpenSSL werden neue Chiffren eingeführt und die Unterstützung für ältere entfernt. Behalten Sie Ihre EC2 AL2 Instanz bei up-to-date, achten Sie auf Sicherheitsankündigungen von OpenSSL und achten Sie auf Berichte über neue Sicherheitslücken in der Fachpresse.

Fehlerbehebung

- Mein Apache-Webserver startet erst, wenn ich ein Passwort eingebe

  Dieses Verhalten wird erwartet, wenn Sie einen verschlüsselten, passwortgeschützten privaten Serverschlüssel installiert haben.

Sie können die Verschlüsselungs- und Passwortanforderung vom Schlüssel entfernen. Angenommen, Sie haben einen privaten, verschlüsselten RSA-Schlüssel, der `custom.key` im Standardverzeichnis aufgerufen wird, und das zugehörige Passwort lautet, führen Sie die folgenden Befehle auf Ihrer EC2 Instance aus**abcde12345**, um eine unverschlüsselte Version des Schlüssels zu generieren.

```
[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 sollte jetzt starten, ohne Sie zur Eingabe eines Passworts aufzufordern.

- Ich erhalten Fehlermeldungen, wenn ich sudo yum install -y mod_ssl ausführe.

  Wenn Sie die für SSL erforderlichen Pakete installieren, treten möglicherweise Fehler wie die folgenden auf.

  ```
  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
  ```

  Das bedeutet in der Regel, dass Ihre EC2 Instance nicht läuft. AL2 Dieses Tutorial unterstützt nur von einer offiziellen AL2-AMI neu erstellte Instances.

Tutorial: Hosten Sie einen WordPress Blog auf AL2

Die folgenden Verfahren helfen Ihnen bei der Installation, Konfiguration und Sicherung eines WordPress Blogs auf Ihrer AL2 Instance. Dieses Tutorial ist eine gute Einführung EC2 in die Verwendung von Amazon, da Sie die volle Kontrolle über einen Webserver haben, auf dem Ihr WordPress Blog gehostet wird, was bei einem herkömmlichen Hosting-Dienst nicht typisch ist.

Sie sind für das Aktualisieren der Softwarepakete und das Warten der Sicherheitspatches für Ihren Server verantwortlich. Für eine stärker automatisierte WordPress Installation, die keine direkte Interaktion mit der Webserver-Konfiguration erfordert, bietet der CloudFormation Service eine WordPress Vorlage, mit der Sie auch schnell loslegen können. Weitere Informationen

finden Sie unter Erste Schritte im AWS CloudFormation -Benutzerhandbuch. Wenn Sie eine Hochverfügbarkeitslösung mit einer entkoppelten Datenbank benötigen, finden Sie weitere Informationen unter Deployment a High Availability WordPress Website im Developer Guide.AWS Elastic Beanstalk

> **Important**
>
> Diese Verfahren sind für die Verwendung mit vorgesehen. AL2 Weitere Informationen zu anderen Verteilungen finden Sie in der jeweiligen Dokumentation. Zahlreiche Schritte in diesem Tutorial funktionieren auf Ubuntu-Instances nicht. Hilfe zur Installation WordPress auf einer Ubuntu-Instanz finden Sie WordPressin der Ubuntu-Dokumentation. Sie können diese Aufgabe auch auf Amazon Linux-, macOS- oder Unix-Systemen ausführen. CodeDeploy

Themen

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie eine AL2 Instanz mit einem funktionierenden Webserver mit PHP- und Datenbankunterstützung (entweder MySQL oder MariaDB) gestartet haben, indem Sie alle Schritte unter ausgeführt haben. Tutorial: Installieren Sie einen LAMP-Server auf AL2 Dieses Tutorial enthält auch Schritte zum Konfigurieren einer Sicherheitsgruppe, um HTTP- und HTTPS-Datenverkehr zuzulassen, sowie mehrere Schritte zum Sicherstellen, dass die Dateiberechtigungen für Ihren Webserver richtig festgelegt sind. Informationen zum Hinzufügen von Regeln zu Ihrer Sicherheitsgruppe finden Sie unter Regeln zu einer Sicherheitsgruppe hinzufügen.

Wir empfehlen dringend, dass Sie der Instance, die Sie zum Hosten eines WordPress Blogs verwenden, eine Elastic IP-Adresse (EIP) zuordnen. Dies verhindert, dass die öffentliche DNS-Adresse für Ihre Instance geändert und Ihre Installation beschädigt wird. Wenn Sie einen Domain-Namen besitzen und für Ihren Blog verwenden möchten, können Sie den DNS-Eintrag für den Domain-Namen so aktualisieren, dass er auf Ihre EIP-Adresse verweist (wenden Sie sich an Ihre Domain-Namen-Registrierungsstelle, wenn Sie dabei Hilfe benötigen). Sie können eine EIP-Adresse

kostenlos mit einer aktiven Instance verknüpfen. Weitere Informationen finden Sie unter Elastic IP-Adressen im EC2 Amazon-Benutzerhandbuch.

Wenn Sie noch keinen Domain-Namen für Ihren Blog haben, können Sie einen Domain-Namen bei Route 53 registrieren und die EIP-Adresse Ihrer Instance mit Ihrem Domain-Namen verknüpfen. Weitere Informationen finden Sie unter Registrieren von Domain-Namen mithilfe von Amazon Route 53 im Entwicklerhandbuch für Amazon Route 53.

Installieren WordPress

Option: Abschließen dieses Tutorials mit Automation

Um dieses Tutorial mit AWS Systems Manager Automatisierung anstelle der folgenden Aufgaben abzuschließen, führen Sie das Automatisierungsdokument aus.

Connect zu Ihrer Instance her und laden Sie das WordPress Installationspaket herunter.

Um das WordPress Installationspaket herunterzuladen und zu entpacken

1. Laden Sie das neueste WordPress Installationspaket mit dem wget Befehl herunter. Mit dem folgenden Befehl sollte immer die aktuelle Version heruntergeladen werden.

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

2. Extrahieren Sie das Installationspaket. Der Installationsordner wird in einem Ordner namens extrahier `wordpress`.

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

Um einen Datenbankbenutzer und eine Datenbank für Ihre WordPress Installation zu erstellen

Ihre WordPress Installation muss Informationen wie Blogbeiträge und Benutzerkommentare in einer Datenbank speichern. Mit diesem Verfahren können Sie eine Datenbank für Ihren Blog und einen Benutzer mit der Berechtigung zum Lesen und Speichern von Informationen in dieser Datenbank erstellen.

1. Starten des Datenbankservers.

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

2. Melden Sie sich auf dem Datenbankserver als `root`-Benutzer an. Geben Sie Ihr Datenbank-`root`-Passwort ein, wenn Sie dazu aufgefordert werden; dieses kann sich von Ihrem `root`-Systempasswort unterscheiden oder sogar leer bleiben, wenn Sie Ihren Datenbankserver nicht gesichert haben.

   Wenn Sie Ihren Datenbankserver noch nicht gesichert haben, ist es wichtig, dass Sie diesen Schritt durchführen. Weitere Informationen finden Sie unter Sichern des MariaDB-Servers (AL2).

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

3. Erstellen Sie einen Benutzer und ein Passwort für Ihre MySQL-Datenbank. Ihre WordPress Installation verwendet diese Werte, um mit Ihrer MySQL-Datenbank zu kommunizieren.

   Achten Sie darauf, ein sicheres Passwort für Ihren Benutzer zu erstellen. Verwenden Sie keine einfachen Anführungszeichen (') in Ihrem Passwort, da diese den vorhergehenden Befehl beschädigen. Verwenden Sie kein bereits vorhandenes Passwort und speichern Sie das Passwort an einem sicheren Ort.

   Geben Sie den folgenden Befehl ein, wobei Sie einen eindeutigen Benutzernamen und ein eindeutiges Passwort einsetzen.

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

4. Erstellen Sie Ihre Datenbank. Geben Sie Ihrer Datenbank einen aussagekräftigen Namen wie `wordpress-db`.

   > **Note**
   >
   > Die Satzzeichen um den Datenbanknamen im folgenden Befehl heißen „einfache umgekehrte Anführungszeichen“. Die Taste für das einfache umgekehrte Anführungszeichen (`) befindet sich auf einer Standardtastatur in der Regel oberhalb der Tab-Taste. Einfache umgekehrte Anführungszeichen sind nicht immer erforderlich, sie ermöglichen Ihnen jedoch die Verwendung von Zeichen in Datenbanknamen, die andernfalls nicht zulässig wären, z. B. Bindestriche.

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

5. Gewähren Sie dem WordPress Benutzer, den Sie zuvor erstellt haben, die vollen Rechte für Ihre Datenbank.

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

6. Löschen Sie die Datenbankrechte, damit alle Ihre Änderungen übernommen werden.

```
FLUSH PRIVILEGES;
```

7. Beenden Sie den `mysql`-Client.

```
exit
```

So erstellen und bearbeiten Sie die Datei „wp-config.php“

Der WordPress Installationsordner enthält eine Beispielkonfigurationsdatei mit dem Namen`wp-config-sample.php`. In diesem Verfahren kopieren und bearbeiten Sie diese Datei, um sie an Ihre individuelle Konfiguration anzupassen.

1. Kopieren Sie die Datei `wp-config-sample.php` in eine Datei namens `wp-config.php`. Dadurch wird eine neue Konfigurationsdatei erstellt und die Originalversion der Beispieldatei als Sicherung aufbewahrt.

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

2. Bearbeiten Sie die Datei `wp-config.php` mit Ihrem bevorzugten Texteditor (z. B. nanooder vim) und geben Sie Werte für Ihre Installation ein. Falls Sie keinen bevorzugten Texteditor haben, ist `nano` für den Einstieg geeignet.

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

   a. Suchen Sie die Zeile, die `DB_NAME` definiert und ändern Sie `database_name_here` in den Namen der Datenbank, die Sie in Step 4 von Um einen Datenbankbenutzer und eine Datenbank für Ihre WordPress Installation zu erstellen erstellt haben.

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

b. Suchen Sie die Zeile, die DB_USER definiert und ändern Sie `username_here` in den Namen des Datenbankbenutzers, den Sie in Step 3 von Um einen Datenbankbenutzer und eine Datenbank für Ihre WordPress Installation zu erstellen erstellt haben.

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

c. Suchen Sie die Zeile, die DB_PASSWORD definiert und ändern Sie `password_here` in das sichere Passwort, das Sie in Step 3 von Um einen Datenbankbenutzer und eine Datenbank für Ihre WordPress Installation zu erstellen erstellt haben.

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

d. Suchen Sie den Abschnitt `Authentication Unique Keys and Salts`. Diese KEY und SALT Werte bieten eine Verschlüsselungsebene für die Browser-Cookies, die WordPress Benutzer auf ihren lokalen Computern speichern. Grundsätzlich wird Ihre Website durch das Hinzufügen langer, zufälliger Werte sicherer. Besuchen Sie https://api.wordpress. org/secret-key/1.1/salt/, um nach dem Zufallsprinzip eine Reihe von Schlüsselwerten zu generieren, die Sie kopieren und in Ihre `wp-config.php` Datei einfügen können. Zum Einfügen von Text in ein PuTTY-Terminal platzieren Sie den Mauszeiger dort, wo der Text eingefügt werden soll, und klicken mit der rechten Maustaste innerhalb des PuTTY-Terminals.

Weitere Informationen zu Sicherheitsschlüsseln finden Sie unter https://wordpress. org/support/article/editing-wp-config-php/#security -keys.

> **Note**
>
> Die folgenden Werte dienen nur als Beispiel; verwenden Sie diese Werte nicht für Ihre Installation.

```
define('AUTH_KEY',         ' #U$$+[RXN8:b^-L 0(WU_+ c+WFkI~c]o]-bHw+)/
Aj[wTwSiZ<Qb[mghEXcRh-');
define('SECURE_AUTH_KEY',  'Zsz._P=l/|y.Lq)XjlkwS1y5NJ76E6EJ.AV0pCKZZB,*~*r ?
6OP$eJT@;+(ndLg');
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',        'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:?0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
```

```
define('AUTH_SALT',        'C$DpB4Hj[JK:?{ql`sRVa:{:7yShy(9A@5wg+`JJVb1fk%_-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.${+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q1O-bp28EKv');
define('LOGGED_IN_SALT',   ';j{00P*owZf)kVD+FVLn-~ >.|Y%Ug4#I^*LVd9QeZ^&XmK|
e(76miC+&W&+^0P/');
define('NONCE_SALT',       '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/,.6[=UK<J_y9?JWG');
```

e. Speichern Sie die Datei und beenden Sie den Texteditor.

Um Ihre WordPress Dateien im Apache Document Root zu installieren

- Nachdem Sie den Installationsordner entpackt, eine MySQL-Datenbank und einen MySQL-Benutzer erstellt und die WordPress Konfigurationsdatei angepasst haben, können Sie Ihre Installationsdateien in den Dokumentenstamm Ihres Webservers kopieren, damit Sie das Installationsskript ausführen können, das Ihre Installation abschließt. Der Speicherort dieser Dateien hängt davon ab, ob Ihr WordPress Blog im eigentlichen Stammverzeichnis Ihres Webservers (z. B.*my.public.dns.amazonaws.com*) oder in einem Unterverzeichnis oder Ordner unter dem Stammverzeichnis (z. B.) verfügbar sein soll. *my.public.dns.amazonaws.com/blog*
  - Wenn Sie es im Stammverzeichnis Ihres Dokuments ausführen WordPress möchten, kopieren Sie den Inhalt des WordPress-Installationsverzeichnisses (aber nicht das Verzeichnis selbst) wie folgt:

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

  - Wenn Sie in einem alternativen Verzeichnis unter dem Dokumentenstamm ausführen möchten WordPress , erstellen Sie zuerst dieses Verzeichnis und kopieren Sie dann die Dateien dorthin. In diesem Beispiel WordPress wird von dem Verzeichnis aus ausgeführt`blog`:

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

> **Important**
>
> Wenn Sie nicht umgehend mit dem nächsten Verfahren fortfahren, beenden Sie aus Sicherheitsgründen den Apache-Webserver (`httpd`) jetzt. Nachdem Sie Ihre Installation in das Apache Document Root verschoben haben, ist das WordPress Installationsskript ungeschützt und ein Angreifer könnte sich Zugriff auf Ihr Blog verschaffen, wenn der Apache-Webserver läuft. Zum Beenden des Apache-Webservers geben Sie den Befehl sudo systemctl stop httpd. Wenn Sie mit dem nächsten Verfahren fortfahren, müssen Sie den Apache-Webserver nicht beenden.

Um die Verwendung von WordPress Permalinks zu ermöglichen

WordPress Permalinks müssen `.htaccess` Apache-Dateien verwenden, um ordnungsgemäß zu funktionieren. Dies ist jedoch unter Amazon Linux standardmäßig nicht aktiviert. Verwenden Sie dieses Verfahren, um alle Überschreibungen im Dokumenten-Stammverzeichnis von Apache zuzulassen.

1. Öffnen Sie die Datei `httpd.conf` mit einem Texteditor Ihrer Wahl (z. B. nano oder vim). Falls Sie keinen bevorzugten Texteditor haben, ist `nano` für den Einstieg geeignet.

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

2. Suchen Sie den Abschnitt, der mit beginn `<Directory "/var/www/html">`.

   ```
   <Directory "/var/www/html">
       #
       # Possible values for the Options directive are "None", "All",
       # or any combination of:
       #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
       #
       # Note that "MultiViews" must be named *explicitly* --- "Options All"
       # doesn't give it to you.
       #
       # The Options directive is both complicated and important.  Please see
       # http://httpd.apache.org/docs/2.4/mod/core.html#options
       # for more information.
       #
       Options Indexes FollowSymLinks

       #
   ```

```
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None

    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>
```

3. Ändern Sie die Zeile `AllowOverride None` im Abschnitt oben in `AllowOverride All`.

> **Note**
>
> Diese Datei enthält mehrere `AllowOverride`-Zeilen; achten Sie unbedingt darauf, die Zeile im Abschnitt `<Directory "/var/www/html">` zu ändern.

```
AllowOverride All
```

4. Speichern Sie die Datei und beenden Sie den Text-Editor.

Um die PHP-Grafikbibliothek zu installieren auf AL2

Mit der GD-Bibliothek für PHP können Sie Bilder bearbeiten. Installieren Sie diese Bibliothek wie folgt, wenn Sie das Header-Image für Ihren Blog zuschneiden müssen. Für die Version phpMyAdmin , die Sie installieren, ist möglicherweise eine bestimmte Mindestversion dieser Bibliothek erforderlich (z. B. Version 7.2).

Verwenden Sie den folgenden Befehl, um die PHP-Grafikzeichnungsbibliothek auf zu installieren AL2. Wenn Sie beispielsweise php7.2 im amazon-linux-extras Rahmen der Installation des LAMP-Stacks installiert haben, installiert dieser Befehl Version 7.2 der PHP-Grafikzeichnungsbibliothek.

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

Verwenden Sie den folgenden Befehl, um die installierte Version zu überprüfen:

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

Das Folgende ist eine Beispielausgabe:

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

So beheben Sie Probleme mit den Dateizugriffsberechtigungen für den Apache-Webserver

Für einige der verfügbaren Funktionen ist Schreibzugriff auf das Apache-Dokumentenstammverzeichnis WordPress erforderlich (z. B. das Hochladen von Medien über die Administrationsbildschirme). Falls Sie dies noch nicht getan haben, wenden Sie die folgenden Gruppenmitgliedschaften und -berechtigungen an (wie in der Tutorial: Installieren Sie einen LAMP-Server auf AL2 ausführlicher beschrieben).

1. Machen Sie den `/var/www`-Benutzer zum Eigentümer der Datei `apache` und ihrer Inhalte.

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

2. Machen Sie die `/var/www`-Gruppe zum Eigentümer der Datei `apache` und ihrer Inhalte.

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

3. Ändern Sie die Verzeichnisberechtigungen von `/var/www` und deren Unterverzeichnissen, indem Sie Schreibberechtigungen für die Gruppe hinzufügen und die Gruppen-ID für zukünftige Unterverzeichnisse einrichten.

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

4. Ändern Sie die Dateiberechtigungen von `/var/www` und deren Unterverzeichnissen rekursiv.

   ```
   [ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
   ```

   > **Note**
   >
   > Wenn Sie beabsichtigen, ihn auch WordPress als FTP-Server zu verwenden, benötigen Sie hier großzügigere Gruppeneinstellungen. Bitte lesen Sie die empfohlenen Schritte und Sicherheitseinstellungen unter, WordPress um dies zu erreichen.

5. Starten Sie den Apache-Webserver neu, damit die neue Gruppe und die neuen Berechtigungen übernommen werden.

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

Führen Sie das WordPress Installationsskript mit aus AL2

Sie sind bereit zur Installation WordPress. Welche Befehle zu verwenden sind, ist vom Betriebssystem abhängig. Die Befehle in diesem Verfahren sind für die Verwendung mit bestimmt AL2.

1. Stellen Sie mit dem Befehl systemctl sicher, dass die `httpd`- und Datenbankdienste bei jedem Systemstart gestartet werden.

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

2. Überprüfen Sie, ob der Datenbankserver ausgeführt wird.

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

   Wenn der Datenbankdienst nicht ausgeführt wird, starten Sie ihn.

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

3. Überprüfen Sie, ob Ihr Apache-Webserver (`httpd`) ausgeführt wird.

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

   Wenn der `httpd`-Dienst nicht ausgeführt wird, starten Sie ihn.

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

4. Geben Sie in einem Webbrowser die URL Ihres WordPress Blogs ein (entweder die öffentliche DNS-Adresse für Ihre Instance oder die Adresse, gefolgt vom `blog` Ordner). Sie sollten das WordPress Installationsskript sehen. Geben Sie die für die WordPress Installation erforderlichen Informationen ein. Klicken Sie auf Installieren WordPress, um die Installation abzuschließen. Weitere Informationen finden Sie unter Schritt 5: Ausführen des Installationsskripts auf der WordPress Website.
   ```

Nächste Schritte

Nachdem Sie Ihren WordPress Blog getestet haben, sollten Sie erwägen, seine Konfiguration zu aktualisieren.

Verwenden eines benutzerdefinierten Domain-Namens

Wenn der EIP-Adresse Ihrer EC2 Instanz ein Domainname zugeordnet ist, können Sie Ihren Blog so konfigurieren, dass dieser Name anstelle der EC2 öffentlichen DNS-Adresse verwendet wird. Weitere Informationen finden Sie unter Ändern der Site-URL auf der WordPress Website.

Konfigurieren Ihres Blogs

Sie können Ihren Blog für die Verwendung verschiedener Designs und Plugins konfigurieren, um Ihren Lesern eine persönlich angepasste Umgebung zu bieten. Bisweilen kann der Installationsprozess jedoch fehlschlagen und zum Verlust des gesamten Blogs führen. Wir empfehlen dringend, eine Amazon Machine Image (AMI)-Sicherung Ihrer Instance zu erstellen, bevor Sie versuchen, Designs oder Plug-Ins zu installieren, damit Sie Ihren Blog wiederherstellen können, falls bei der Installation ein Fehler auftritt. Weitere Informationen finden Sie unter Erstellen Sie Ihr eigenes AMI.

Erhöhen der Kapazität

Wenn Ihr WordPress Blog immer beliebter wird und Sie mehr Rechenleistung oder Speicherplatz benötigen, sollten Sie die folgenden Schritte in Betracht ziehen:

- Erweitern Sie den Speicherplatz auf Ihrer Instance. Weitere Informationen finden Sie unter Amazon EBS Elastic Volumes im Amazon-EBS-Benutzerhandbuch.
- Verschieben Sie Ihre MySQL-Datenbank zu Amazon RDS, um die Möglichkeit zur einfachen Skalierung dieses Services zu nutzen.

Verbesserung der Netzwerkleistung Ihres Internetverkehrs

Wenn Sie erwarten, dass Ihr Blog den Traffic von Nutzern auf der ganzen Welt steigern wird, sollten Sie AWS Global Accelerator in Betracht ziehen. Global Accelerator hilft Ihnen dabei, die Latenz zu senken, indem es die Leistung des Internetverkehrs zwischen den Client-Geräten Ihrer Benutzer und Ihrer WordPress Anwendung, auf der ausgeführt wird, verbessert AWS. Global Accelerator nutzt das AWS globale Netzwerk, um den Datenverkehr an einen funktionierenden Anwendungsendpunkt in der AWS Region weiterzuleiten, die dem Client am nächsten ist.

Erfahren Sie mehr über WordPress

Informationen dazu WordPress finden Sie in der WordPress Codex-Hilfedokumentation unter http://codex.wordpress.org/.

Weitere Informationen zur Problembehandlung bei Ihrer Installation finden Sie unter Häufige Installationsprobleme.

Informationen dazu, wie Sie Ihr WordPress Blog sicherer machen können, finden Sie unter Hardening WordPress.

Informationen dazu, wie Sie Ihr WordPress Blog behalten up-to-date, finden Sie unter Aktualisieren WordPress.

Hilfe! Mein öffentlicher DNS-Name hat sich geändert und jetzt funktioniert mein Blog nicht mehr.

Ihre WordPress Installation wird automatisch mit der öffentlichen DNS-Adresse für Ihre EC2 Instance konfiguriert. Wenn Sie die Instance beenden und neu starten, ändert sich die öffentliche DNS-Adresse (sofern sie nicht mit einer Elastic IP-Adresse verknüpft ist) und Ihr Blog funktioniert nicht mehr, da er auf Ressourcen verweist, die nicht mehr existieren (oder einer anderen EC2 Instance zugewiesen sind). Eine detailliertere Beschreibung des Problems und mehrere mögliche Lösungen finden Sie unter Ändern der Site-URL.

Wenn dies bei Ihrer WordPress Installation passiert ist, können Sie Ihr Blog möglicherweise mit dem folgenden Verfahren wiederherstellen, bei dem die wp-cli Befehlszeilenschnittstelle für verwendet wird WordPress.

Um die URL Ihrer WordPress Website mit dem zu ändern wp-cli

1. Stellen Sie mit SSH eine Connect zu Ihrer EC2 Instance her.
2. Notieren Sie die alte und die neue Website-URL für Ihre Instance. Bei der alten Site-URL handelt es sich wahrscheinlich um den öffentlichen DNS-Namen für Ihre EC2 Instance, als Sie sie installiert haben WordPress. Die neue Site-URL ist der aktuelle öffentliche DNS-Name für Ihre EC2 Instance. Wenn Sie nicht sicher sind, was Ihre alte Website-URL ist, können Sie sie mit dem folgenden Befehl mithilfe von curl ermitteln.

   ```
   [ec2-user ~]$ curl localhost | grep wp-content
   ```

In der Ausgabe, die folgendermaßen aussieht (alte Website-URL in rot) sollten Referenzen auf Ihren alten öffentlichen DNS-Namen enthalten sein:

```
<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. Laden Sie das wp-cli mit dem folgenden Befehl herunter.

```
[ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/
phar/wp-cli.phar
```

4. Suchen und ersetzen Sie die alte Site-URL in Ihrer WordPress Installation durch den folgenden Befehl. Ersetzen Sie Ihre EC2 Instanz und den Pfad URLs zu Ihrer WordPress Installation durch die alte und die neue Site (normalerweise `/var/www/html` oder`/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. Geben Sie in einem Webbrowser die neue Site-URL Ihres WordPress Blogs ein, um zu überprüfen, ob die Website wieder ordnungsgemäß funktioniert. Ist dies nicht der Fall, finden Sie weitere Informationen unter Ändern der Site-URL und Häufige Installationsprobleme.

Amazon Linux 2 außerhalb von Amazon verwenden EC2

Die AL2 Container-Images können in kompatiblen Container-Laufzeitumgebungen ausgeführt werden.

AL2 kann auch als virtualisierter Gast ausgeführt werden, wenn es nicht direkt auf Amazon EC2 ausgeführt wird.

> **Note**
>
> Die Konfiguration der AL2 Bilder unterscheidet sich von AL2 023.
> Stellen Sie bei der Migration zu AL2 023 sicher, dass Sie Amazon Linux 2023 außerhalb von Amazon verwenden lesen EC2 und Ihre Konfiguration so anpassen, dass sie mit AL2 023 kompatibel ist.

AL2 Als virtuelle Maschine vor Ort ausführen

Verwenden Sie die Images der AL2 virtuellen Maschine (VM) für die Entwicklung und das Testen vor Ort. Wir bieten für jede der unterstützten Virtualisierungsplattformen ein anderes AL2 VM-Image an. Sie können die Liste der unterstützten Plattformen auf der Seite Amazon-Linux-2-Images für virtuelle Maschinen sehen.

Gehen Sie wie folgt vor, um die Images der AL2 virtuellen Maschine mit einer der unterstützten Virtualisierungsplattformen zu verwenden:

- Schritt 1: Vorbereiten des seed.iso-StartImages
- Schritt 2: Herunterladen des AL2-VM-Abbilds
- Schritt 3: Starten und Verbinden mit der neuen VM

Schritt 1: Vorbereiten des `seed.iso`-StartImages

Das `seed.iso`-Start-Image enthält die Erstkonfigurationsinformationen, die zum Starten Ihrer neuen VM benötigt werden, wie Netzwerkkonfiguration, Hostname und Benutzerdaten.

> **Note**
>
> Das `seed.iso`-Start-Image enthält nur die Konfigurationsinformationen, die zum Starten der VM benötigt werden. Die AL2 Betriebssystemdateien sind nicht enthalten.

Zum Erstellen des `seed.iso`-Start-Images benötigen Sie zwei Konfigurationsdateien:

- `meta-data` – Diese Datei enthält den Hostnamen und statische Netzwerkeinstellungen für die VM.
- `user-data` – Diese Datei konfiguriert Benutzerkonten und gibt deren Passwörter, Schlüsselpaare und Zugriffsmechanismen an. Standardmäßig erstellt das AL2 VM-Image ein `ec2-user` Benutzerkonto. Sie verwenden die `user-data`-Konfigurationsdatei zum Festlegen des Passworts für das Standard-Benutzerkonto.

So erstellen Sie den **`seed.iso`**-Startdatenträger:

1. Erstellen Sie einen neuen Ordner mit dem Namen `seedconfig` und navigieren Sie dorthin.
2. Erstellen Sie die `meta-data`-Konfigurationsdatei.
   a. Erstellen Sie eine neue Datei mit dem Namen `meta-data`.
   b. Öffnen Sie die Datei `meta-data` mit Ihrem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

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

   *vm_hostname*Ersetzen Sie es durch einen VM-Hostnamen Ihrer Wahl und konfigurieren Sie die Netzwerkeinstellungen nach Bedarf.

   c. Speichern und schließen Sie die `meta-data`-Konfigurationsdatei.

Für ein Beispiel einer `meta-data`-Konfigurationsdatei, die einen VM-Host-Namen (`amazonlinux.onprem`) angibt, die Standardnetzwerkschnittstelle (`eth0`) konfiguriert and statische IP-Adressen für die erforderlichen Netzwerkgeräte festlegt, vgl. die Seed.iso-Beispieldatei..

3. Erstellen Sie die `user-data`-Konfigurationsdatei.

   a. Erstellen Sie eine neue Datei mit dem Namen `user-data`.

   b. Öffnen Sie die Datei `user-data` mit Ihrem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

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

   *plain_text_password*Ersetzen Sie es durch ein Passwort Ihrer Wahl für das `ec2-user` Standardbenutzerkonto.

   c. (Optional) Standardmäßig wendet cloud-init bei jedem VM-Start Netzwerkeinstellungen an. Fügen Sie Folgendes hinzu, um zu verhindern, dass cloud-init bei jedem Start Netzwerkeinstellungen anwendet, und um die beim ersten Start angewandten Netzwerkeinstellungen beizubehalten.

```
# 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. Speichern und schließen Sie die `user-data`-Konfigurationsdatei.

Sie können zusätzliche Benutzerkonten erstellen und deren Zugriffsmechanismen, Passwörter und Schlüsselpaare angeben. Weitere Informationen zu den unterstützten Anweisungen finden Sie unter Modulreferenz. Für eine `user-data`-Beispieldatei, die drei zusätzliche Benutzer erstellt und ein benutzerdefiniertes Passwort für das Standard-`ec2-user`-Benutzerkonto angibt, vgl. die Seed.iso-Beispieldatei.

4. Erstellen Sie das `seed.iso`-Start-Image mithilfe der `meta-data`- und `user-data`-Konfigurationsdateien.

   Verwenden Sie für Linux ein Tool wie genisoimage. Navigieren Sie zum Ordner `seedconfig` und führen Sie den folgenden Befehl aus.

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

   Verwenden Sie für macOS ein Tool wie hdiutil. Wechseln Sie aus dem Ordner `seedconfig` zur nächsthöheren Ebene und führen Sie den folgenden Befehl aus.

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

Schritt 2: Herunterladen des AL2-VM-Abbilds

Wir bieten für jede der unterstützten Virtualisierungsplattformen ein anderes AL2 VM-Image an. Sie können die Liste der unterstützten Plattformen anzeigen und das korrekte VM-Image für die von Ihnen gewählte Plattform auf der Seite Amazon-Linux-2-Images für virtuelle Maschinen sehen.

Schritt 3: Starten und Verbinden mit der neuen VM

Um Ihre neue VM zu booten und eine Verbindung zu ihr herzustellen, benötigen Sie das `seed.iso` Boot-Image (erstellt in Schritt 1) und ein AL2 VM-Image (heruntergeladen in Schritt 2). Die Schritte variieren je nach Ihrer ausgewählten VM-Plattform.

VMware vSphere

Das VM-Image für VMware wird im OVF-Format zur Verfügung gestellt.

Um die VM mit VMware vSphere zu starten

1. Erstellen Sie einen neuen Datenspeicher für die `seed.iso`-Datei oder fügen Sie sie zu einem vorhandenen Datenspeicher hinzu.
2. Stellen Sie die OVF-Vorlage bereit, starten Sie die VM jedoch noch nicht.
3. Klicken Sie im Navigator-Bedienfeld mit der rechten Maustaste auf die neue virtuelle Maschine und wählen Sie Einstellungen bearbeiten aus.
4. Wählen Sie auf der Registerkarte Virtuelle Hardware für Neues Gerät die Option CD/DVD-Laufwerk und aus wählen Sie dann Hinzufügen aus.
5. Wählen Sie für New CD/DVD Drive die Option Datastore ISO File aus. Wählen Sie den Datenspeicher aus, dem Sie die `seed.iso`-Datei hinzugefügt haben, navigieren Sie zu der `seed.iso`-Datei, wählen Sie sie aus und wählen Sie dann OK aus.
6. Wählen Sie für New CD/DVD Drive die Option Connect und dann OK aus.

Nachdem Sie den Datenspeicher mit der VM verknüpft haben, sollten Sie ihn booten können.

KVM

So starten Sie die VM mit KVM

1. Öffnen Sie den Assistenten Neue VM erstellen.
2. Wählen Sie für Schritt 1 die Option Vorhandenes Disk-Image importieren aus.
3. Navigieren Sie für Schritt 2 zum VM-Image und wählen Sie es aus. Wählen Sie bei OS type (Betriebssystemtyp) und Version Linux bzw. Red Hat Enterprise Linux 7.0.
4. Geben Sie für Schritt 3 die Größe des Arbeitsspeichers und die Anzahl der CPUs zu verwendenden RAMs an.
5. Geben Sie für Schritt 4 einen Namen für die neue VM ein, wählen Sie Konfiguration vor der Installation anpassen aus und wählen Sie Fertig stellen aus.
6. Wählen Sie im Konfigurationsfenster für die VM die Option Hardware hinzufügen aus.
7. Wählen Sie im Fenster Neue virtuelle Hardware hinzufügen die Option Speicher aus.
8. Wählen Sie in der Speicherkonfiguration Benutzerdefinierter Speicher auswählen oder erstellen aus. Wählen Sie für Gerätetyp CD-ROM-Gerät aus. Wählen Sie Verwalten, Lokal durchsuchen aus und navigieren Sie zur `seed.iso`-Datei und wählen Sie sie aus. Klicken Sie auf Finish.
9. Wählen Sie Installation beginnen aus.

Oracle VirtualBox

Um die VM mit Oracle zu starten VirtualBox

1. Öffnen Sie Oracle VirtualBox und wählen Sie Neu.
2. Geben Sie unter Name einen beschreibenden Namen für die virtuelle Maschine ein und wählen Sie unter Type (Typ) und Version Linux bzw. Red Hat (64-bit) aus. Klicken Sie auf Continue.
3. Geben Sie unter Speichergröße, die Größe des Speichers an, die der virtuellen Maschine zugewiesen werden soll, und klicken Sie dann auf Weiter.
4. Wählen Sie für Hard disk (Festplatte) die Option Use an existing virtual hard disk file (Eine vorhandene virtuelle Festplattendatei verwenden), navigieren Sie zum VM-Image, öffnen Sie das VM-Image, und klicken Sie dann auf Erstellen.
5. Bevor Sie die VM starten, müssen Sie die `seed.iso`-Datei in das virtuelle optische Laufwerk der virtuellen Maschine laden:

   a. Wählen Sie die neue VM aus, wählen Sie Einstellungen und dann Speicher aus.

   b. Wählen Sie in der Liste Storage Devices (Speichergeräte) unter Controller: IDE das leere optische Laufwerk aus.

   c. Wählen Sie im Abschnitt Attribute für das optische Laufwerk die Schaltfläche „Durchsuchen“ aus, wählen Sie Virtuelle optische Datenträgerdatei auswählen aus und wählen Sie dann die `seed.iso`-Datei aus. Klicken Sie auf OK, um die Änderungen anzuwenden und die Einstellungen zu schließen.

Nachdem Sie die `seed.iso`-Datei dem virtuellen optischen Laufwerk hinzugefügt haben, sollten Sie die VM starten können.

Microsoft Hyper-V

Das VM-Image für Microsoft Hyper-V wird in eine ZIP-Datei komprimiert. Sie müssen den Inhalt der ZIP-Datei extrahieren.

So starten Sie die VM mit Microsoft Hyper-V

1. Öffnen Sie den New Virtual Machine Wizard (neuen Assistenten für virtuelle Maschinen).
2. Wenn Sie aufgefordert werden, eine Generation auszuwählen, wählen Sie Generation 1 aus.

3. Wenn Sie aufgefordert werden, den Netzwerkadapter zu konfigurieren, wählen Sie für Verbindung Extern aus.
4. Wenn Sie aufgefordert werden, eine virtuelle Festplatte zu verbinden, wählen Sie Vorhandene virtuelle Festplatte verwenden aus, wählen Sie Durchsuchen aus und navigieren Sie dann zum VM-Image und wählen Sie das VM-Image aus. Wählen Sie Fertig stellen aus, um die VM zu erstellen.
5. Klicken Sie mit der rechten Maustaste auf die neue VM und wählen Sie Einstellungen aus. Wählen Sie im Fenster Einstellungen unter IDE Controller 1 die Option DVD-Laufwerk aus.
6. Wählen Sie für das DVD-Laufwerk Image-Datei aus, navigieren Sie zur `seed.iso`-Datei und wählen Sie sie aus.
7. Übernehmen Sie die Änderungen und starten Sie die VM.

Nachdem die VM gestartet wurde, melden Sie sich mit einem der in der `user-data`-Konfigurationsdatei definierten Benutzerkonten an. Nachdem Sie sich zum ersten Mal angemeldet haben, können Sie anschließend das `seed.iso`-Boot-Image von der VM trennen.

Identifizieren von Amazon Linux-Instances und -Versionen

Es kann wichtig sein, feststellen zu können, um welche Linux-Distribution es sich handelt und um welche Version dieser Distribution es sich bei einem Betriebssystem-Image oder einer Instance handelt. Amazon Linux bietet Mechanismen, um Amazon Linux von anderen Linux-Distributionen zu unterscheiden und um zu ermitteln, um welche Version von Amazon Linux es sich bei dem Image handelt.

In diesem Abschnitt werden die verschiedenen Methoden, die verwendet werden können, und ihre Einschränkungen sowie einige Anwendungsbeispiele behandelt.

Themen

Unter Verwendung des `os-release` Standards

Amazon Linux entspricht dem `os-release`Standard zur Identifizierung von Linux-Distributionen. Diese Datei enthält maschinenlesbare Informationen zur Betriebssystemidentifikation und Versionsinformationen.

> **Note**
>
> Der Standard schreibt vor, dass zuerst versucht `/etc/os-release` wird, analysiert zu werden, gefolgt von. `/usr/lib/os-release` Es sollte darauf geachtet werden, dass der Standard in Bezug auf Dateinamen und Pfade eingehalten wird.

Themen

Die wichtigsten Unterschiede bei der Identifizierung

`os-release`Das finden Sie unter`/etc/os-release`, und falls das nicht vorhanden ist, unter`/usr/lib/os-release`. Vollständige Informationen finden Sie in der `os-release`Norm.

Die zuverlässigste Methode, um festzustellen, ob auf einer Instance Amazon Linux ausgeführt wird, besteht darin, das `ID` Feld einzucheckenos-release.

Die zuverlässigste Methode, um zwischen Versionen zu unterscheiden, besteht darin, das `VERSION_ID` Feld wie folgt einzucheckenos-release:

- Amazon Linux AMI: `VERSION_ID` enthält eine datumsbasierte Version (z. B.) `2018.03`
- AL2: `VERSION_ID="2"`
- AL2023: `VERSION_ID="2023"`

> **Note**
>
> Denken Sie daran, dass `VERSION_ID` es sich um ein maschinenlesbares Feld handelt, das für den programmatischen Gebrauch bestimmt ist, während `PRETTY_NAME` es für die Anzeige durch Benutzer konzipiert ist. Weitere Informationen the section called “Feldtypen” zu Feldtypen finden Sie unter.

Feldtypen: Maschinenlesbar oder menschenlesbar

Die `/etc/os-release` Datei (oder `/usr/lib/os-release` falls `/etc/os-release` nicht vorhanden) enthält zwei Arten von Feldern: maschinenlesbare Felder für den programmatischen Gebrauch und menschenlesbare Felder, die Benutzern präsentiert werden sollen.

Maschinenlesbare Felder

Diese Felder verwenden standardisierte Formate und sind für die Verarbeitung durch Skripte, Paketmanager und andere automatisierte Tools vorgesehen. Sie enthalten nur Kleinbuchstaben, Zahlen und begrenzte Satzzeichen (Punkte, Unterstriche und Bindestriche).

- `ID`— Betriebssystem-ID. Amazon Linux verwendet es `amzn` in allen Versionen und unterscheidet es von anderen Distributionen wie Debian (`debian`), Ubuntu (`ubuntu`) oder Fedora () `fedora`
- `VERSION_ID`— Betriebssystemversion für programmatische Zwecke (z. B.) `2023`

- `ID_LIKE`— Durch Leerzeichen getrennte Liste verwandter Distributionen (z. B.) `fedora`
- `VERSION_CODENAME`— Geben Sie den Codenamen für Skripte frei (z. B.) `karoo`
- `VARIANT_ID`— Varianten-ID für programmatische Entscheidungen
- `BUILD_ID`— Build-ID für Systemabbilder
- `IMAGE_ID`— Image-ID für containerisierte Umgebungen
- `PLATFORM_ID`— Plattform-ID (z. B.) `platform:al2023`

Für Menschen lesbare Felder

Diese Felder sind für die Anzeige durch Benutzer vorgesehen und können Leerzeichen, Groß- und Kleinschreibung sowie beschreibenden Text enthalten. Sie sollten verwendet werden, wenn Betriebssysteminformationen in Benutzeroberflächen dargestellt werden.

- `NAME`— Name des Betriebssystems für die Anzeige (z. B.`Amazon Linux`)
- `PRETTY_NAME`— Vollständiger Betriebssystemname mit Version für die Anzeige (z. B.`Amazon Linux 2023.8.20250721`)
- `VERSION`— Versionsinformationen, die für die Benutzerpräsentation geeignet sind
- `VARIANT`— Name der Variante oder Edition für die Anzeige `Server Edition` (z. B.

Andere Informationsfelder

Diese Felder enthalten zusätzliche Metadaten zum Betriebssystem:

- `HOME_URL`— URL der Projekt-Homepage
- `DOCUMENTATION_URL`— URL der Dokumentation
- `SUPPORT_URL`— URL Support Support-Informationen
- `BUG_REPORT_URL`— URL zur Fehlerberichterstattung
- `VENDOR_NAME`— Name des Anbieters
- `VENDOR_URL`— URL des Anbieters
- `SUPPORT_END`— End-of-support Datum im YYYY-MM-DD Format
- `CPE_NAME`— Gemeinsamer Bezeichner für die Plattformaufzählung
- `ANSI_COLOR`— ANSI-Farbcode für die Terminalanzeige

Verwenden Sie beim Schreiben von Skripten oder Anwendungen, die Amazon Linux programmgesteuert identifizieren müssen, maschinenlesbare Felder wie und. `ID` `VERSION_ID` Wenn Sie Benutzern Betriebssysteminformationen anzeigen, verwenden Sie menschenlesbare Felder wie. `PRETTY_NAME`

Beispiele für **`/etc/os-release`**

Der `/etc/os-release` Dateiinhalt variiert zwischen den Amazon Linux-Versionen:

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/"
```

Vergleich mit anderen Distributionen

Um zu verstehen, wie Amazon Linux in das breitere Linux-Ökosystem passt, vergleichen Sie sein `/etc/os-release` Format mit anderen wichtigen Distributionen:

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
```

Beachten Sie, dass die maschinenlesbaren Felder für eine einheitliche Identifizierung in allen Distributionen sorgen:

- `ID`— Identifiziert das Betriebssystem eindeutig: `amzn` für Amazon Linux, `fedora` für Fedora, `debian` für Debian, `ubuntu` für Ubuntu
- `ID_LIKE`— Zeigt Distributionsbeziehungen: Amazon Linux verwendet `fedora` (AL2023) oder `centos rhel fedora` (AL2), während Ubuntu zeigt, `debian` um auf seine Debian-Herkunft hinzuweisen
- `VERSION_ID`— Stellt maschinenlesbare Versionsinformationen bereit: `2023` für AL2 023, für Fedora, `42` für Debian, für Ubuntu `12` `24.04`

Im Gegensatz dazu sind die menschenlesbaren Felder so konzipiert, dass sie Benutzern angezeigt werden:

- `NAME`— Benutzerfreundlicher Betriebssystemname:`Amazon Linux`,,, `Fedora Linux` `Debian GNU/Linux` `Ubuntu`
- `PRETTY_NAME`— Vollständiger Anzeigename mit Version:`Amazon Linux 2023.8.20250721`,`Fedora Linux 42 (Container Image)`,`Debian GNU/Linux 12 (bookworm)`, `Ubuntu 24.04.2 LTS`
- `VERSION`— Für Menschen lesbare Version mit zusätzlichem Kontext wie Codenamen oder Releasetypen

Verwenden Sie beim Schreiben plattformübergreifender Skripts immer die maschinenlesbaren Felder (`ID`,`VERSION_ID`,`ID_LIKE`) für Logik und Entscheidungen und die menschenlesbaren Felder (`PRETTY_NAME`,) nur zur Anzeige von Informationen für Benutzer. `NAME`

Amazon Linux-spezifisch

Es gibt einige Amazon Linux-spezifische Dateien, anhand derer Amazon Linux und dessen Version identifiziert werden können. Neuer Code sollte den `/etc/os-release` Standard verwenden, um vertriebsübergreifend kompatibel zu sein. Von der Verwendung von Amazon Linux-spezifischen Dateien wird abgeraten.

Themen

Die Datei `/etc/system-release`

Amazon Linux enthält eine `/etc/system-release`-Datei, in der die aktuell installierte Version angegeben ist. Diese Datei wird mithilfe von Paketmanagern aktualisiert und ist unter Amazon Linux Teil des `system-release` Pakets. Während einige andere Distributionen wie Fedora diese Datei ebenfalls haben, ist sie in Debian-basierten Distributionen wie Ubuntu nicht vorhanden.

> **Note**
>
> Die `/etc/system-release` Datei enthält eine für Menschen lesbare Zeichenfolge und sollte nicht programmgesteuert zur Identifizierung eines Betriebssystems oder einer Version verwendet werden. Verwenden Sie stattdessen die maschinenlesbaren Felder in `/etc/os-release` (oder `/usr/lib/os-release` falls nicht `/etc/os-release` vorhanden).

Amazon Linux enthält auch eine maschinenlesbare Version davon`/etc/system-release`, die der Common Platform Enumeration (CPE) -Spezifikation in der Datei entspricht. `/etc/system-release-cpe`

Image-Identifikationsdatei

Jedes Amazon Linux-Image enthält eine eindeutige `/etc/image-id` Datei, die zusätzliche Informationen über das vom Amazon Linux-Team generierte Original-Image enthält. Diese Datei ist spezifisch für Amazon Linux und befindet sich nicht in anderen Linux-Distributionen wie Debian, Ubuntu oder Fedora. Diese Datei enthält die folgenden Informationen über das Image:

- `image_name`,`image_version`, `image_arch` — Werte aus dem Build-Rezept, das zur Erstellung des Images verwendet wurde.
- `image_stamp` – Ein eindeutiger, beliebiger Hexadezimalwert, der bei der Erstellung des Images generiert wurde.
- `image_date`— Die UTC-Zeit der Image-Erstellung im YYYYMMDDhhmmssFormat.

- `recipe_name`, `recipe_id` — Der Name und die ID des Build-Rezepts, das zur Erstellung des Images verwendet wurde.

Beispiele für Amazon Linux-spezifische Dateien

Die folgenden Abschnitte enthalten Beispiele für die Amazon Linux-spezifischen Identifikationsdateien für jede Hauptversion von Amazon Linux.

> **Note**
>
> `/usr/lib/os-release`Sollte in jedem realen Code verwendet werden, wenn die `/etc/os-release` Datei nicht existiert.

AL2023

Die folgenden Beispiele zeigen die Identifikationsdateien für AL2 023.

Beispiel `/etc/image-id` für 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"
```

Beispiel `/etc/system-release` für für AL2 023:

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

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

AL2

Die folgenden Beispiele zeigen die Identifikationsdateien für AL2.

Beispiel `/etc/image-id` für 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"
```

Beispiel `/etc/system-release` für AL2:

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

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

Amazon Linux-AMI

Die folgenden Beispiele zeigen die Identifikationsdateien für Amazon Linux AMI.

Beispiel `/etc/image-id` für 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"
```

Beispiel `/etc/system-release` für Amazon Linux AMI:

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

```
Amazon Linux AMI release 2018.03
```

Beispielcode für die Betriebssystemerkennung

Die folgenden Beispiele zeigen, wie das Betriebssystem und die Version mithilfe der Datei `/etc/os-release` (oder `/usr/lib/os-release` falls `/etc/os-release` nicht vorhanden) programmgesteuert erkannt werden. Diese Beispiele zeigen, wie man zwischen Amazon Linux und anderen Distributionen unterscheidet und wie das `ID_LIKE` Feld verwendet wird, um Distributionsfamilien zu bestimmen.

Das folgende Skript ist in verschiedenen Programmiersprachen implementiert, und jede Implementierung erzeugt dieselbe Ausgabe.

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";
    }
}
```

Wenn das Skript auf verschiedenen Systemen ausgeführt wird, erzeugt es die folgende Ausgabe:

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)
```

AWSIntegration in AL2

AWSBefehlszeilentools

The AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, das eine konsistente Schnittstelle bietet, mit der Sie AWS-Services mithilfe von Befehlen in Ihrer Befehlszeilen-Shell interagieren können. Weitere Informationen finden Sie unter Was ist der? AWS Command Line Interface im AWS Command Line InterfaceBenutzerhandbuch.

AL2 und AL1 haben Version 1 des AWS CLI vorinstalliert. In der aktuellen Version von Amazon Linux, AL2 023, ist Version 2 von AWS CLI vorinstalliert. Weitere Informationen zur Verwendung von AWS CLI on AL2 023 finden Sie unter Erste Schritte mit AL2 023 im Amazon Linux 2023-Benutzerhandbuch.

Erste Schritte mit der Laufzeitprogrammierung

AL2 stellt verschiedene Versionen bestimmter Sprachlaufzeiten bereit. Wir arbeiten mit Upstream-Projekten wie PHP, die mehrere Versionen gleichzeitig unterstützen. Um Informationen zur Installation und Verwaltung dieser Pakete mit Namensversionen zu erhalten, verwenden Sie den `yum` Befehl, um diese Pakete zu suchen und zu installieren. Weitere Informationen finden Sie unter Paket-Repository.

In den folgenden Themen wird beschrieben, wie die einzelnen Sprachen von Runtime funktionieren. AL2

Themen

- CC++, und Fortran in AL2
- Geh rein AL2
- Javain AL2
- Perlin AL2
- PHPin AL2
- Pythonin AL2
- Einrosten AL2

CC++, und Fortran in AL2

AL2 beinhaltet sowohl die GNU Compiler Collection (GCC) als auch das Clang Frontend für. LLVM

Die Hauptversion von GCC wird während der gesamten Lebensdauer von konstant bleiben. AL2 Fehler- und Sicherheitskorrekturen werden möglicherweise auf die Hauptversion zurückportiertGCC, in AL2 der sie mitgeliefert wird.

AL2 Enthält standardmäßig Version 7.3, von der fast alle GCC Pakete erstellt werden. Das `gcc10` Paket stellt GCC 10 in begrenztem Umfang zur Verfügung, wir empfehlen jedoch nicht, GCC 10 zum Erstellen von Paketen zu verwenden.

Die Standard-Compiler-Flags, die gebaut werden, AL2 RPMs beinhalten einige Optimierungs- und Härtungsflags. Wir empfehlen, einige Optimierungs- und Hardening-Flags hinzuzufügen, wenn Sie Ihren eigenen Code damit GCC erstellen.

Die Standard-Compiler- und Optimierungsflags in AL2 023 verbessern das, was in vorhanden ist. AL2

Geh rein AL2

Möglicherweise möchten Sie Ihren eigenen Code, der Goauf Amazon Linux geschrieben wurde, mithilfe einer AL2 mitgelieferten Toolchain erstellen.

Die Go Toolchain wird während der gesamten Lebensdauer von aktualisiert. AL2 Dies kann als Reaktion auf ein beliebiges CVE in der von uns gelieferten Toolchain geschehen oder als Voraussetzung für die Adressierung eines CVE in einem anderen Paket.

Goist eine relativ schnelllebige Programmiersprache. Es kann vorkommen, dass bestehende Anwendungen, in die geschrieben Go wurden, an neue Versionen der Go Toolchain angepasst werden müssen. Weitere Informationen dazu finden Sie Go unter Go1 und die Zukunft der Go Programme.

Zwar AL2 werden im Laufe der Laufzeit neue Versionen der Go Toolchain integriert, diese wird jedoch nicht im Gleichschritt mit den Go Upstream-Versionen erfolgen. Daher ist die Verwendung der unter bereitgestellten Go Toolchain AL2 möglicherweise nicht geeignet, wenn Sie Go Code mit den neuesten Funktionen der Go Sprache und der Standardbibliothek erstellen möchten.

Während der Lebensdauer von AL2 werden frühere Paketversionen nicht aus den Repositorys entfernt. Wenn eine frühere Go Toolchain erforderlich ist, können Sie auf Fehler- und Sicherheitskorrekturen neuerer Go Toolchains verzichten und eine frühere Version aus den Repositorys installieren, indem Sie dieselben Mechanismen verwenden, die für jedes RPM verfügbar sind.

Wenn Sie Ihren eigenen Go Code darauf aufbauen möchten, können AL2 Sie die mitgelieferte Go Toolchain AL2 mit dem Wissen verwenden, dass diese Toolchain im Laufe der Lebensdauer von weiterentwickelt werden kann. AL2

Javain AL2

AL2 bietet mehrere Versionen von Amazon Corretto zur Unterstützung von Java basierten Workloads sowie einige Versionen. OpenJDK Wir empfehlen Ihnen, zu Amazon Corretto zu migrieren, um die Migration auf 023 vorzubereiten. AL2

Corretto ist ein Build des Open Java Development Kit (OpenJDK) mit langfristiger Unterstützung von. Amazon Corretto ist mit dem Java Technical Compatibility Kit (TCK) zertifiziert, um sicherzustellen, dass es dem Java SE-Standard entspricht und aufLinux, Windows und verfügbar ist. macOS

Für Corretto 1.8.0, Corretto 11 und Corretto 17 ist jeweils ein Amazon Corretto-Paket verfügbar.

Jede Corretto-Version in AL2 wird für den gleichen Zeitraum wie die Corretto-Version unterstützt, oder bis zum Lebensende von, je nachdem AL2, was früher eintritt. Weitere Informationen finden Sie im Amazon Corretto FAQs.

Perlin AL2

AL2 stellt Version 5.16 der PerlProgrammiersprache bereit.

PerlModule in AL2

Verschiedene Perl Module sind wie RPMs in verpackt AL2. Obwohl es viele Perl Module gibt RPMs, versucht Amazon Linux nicht, jedes mögliche Perl Modul zu paketieren. Module, die so verpackt sind, wie sie von anderen RPM-Paketen für Betriebssysteme verwendet werden RPMs könnten, sodass Amazon Linux der Sicherstellung, dass sie Sicherheitspatches enthalten, Vorrang vor reinen Funktionsupdates einräumt.

AL2 beinhaltet auch, `CPAN` dass Perl Entwickler den idiomatischen Paketmanager für Module verwenden können. Perl

PHPin AL2

AL2 bietet derzeit zwei vollständig unterstützte Versionen der PHPProgrammiersprache als Teil vonAL2 Extras-Bibliothek. Jede PHP Version wird für denselben Zeitraum wie die PHP Upstream-Version unterstützt, wie unter dem Datum für veraltete Version in aufgeführt. Liste der Amazon Linux 2-Extras

Informationen zur Verwendung von AL2 Extras zur Installation von Anwendungs- und Softwareupdates auf Ihren Instanzen finden Sie unter. AL2 Extras-Bibliothek

Zur Unterstützung der Migration auf AL2 023 sind sowohl PHP 8.1 als auch 8.2 auf AL2 und AL2 023 verfügbar.

> **Note**
>
> AL2 umfasst PHP 7.1, 7.2, 7.3 und 7.4 Zoll. `amazon-linux-extras` Bei all diesen Extras handelt es sich um EOL und es kann nicht garantiert werden, dass zusätzliche Sicherheitsupdates verfügbar sind.
> Informationen darüber, wann die einzelnen Versionen von veraltet PHP sind AL2, finden Sie unter. Liste der Amazon Linux 2-Extras

Migration von früheren 8.x-Versionen PHP

Die PHP Upstream-Community hat eine umfassende Migrationsdokumentation für die Umstellung von PHPPHP 8.1 auf 8.2 zusammengestellt. Es gibt auch eine Dokumentation für die Migration von PHP 8.0 auf 8.1.

AL2 umfasst PHP 8.0, 8.1 und 8.2, was einen effizienten Upgrade-Pfad auf Version AL2 023 ermöglicht. `amazon-linux-extras` Informationen darüber, wann die einzelnen Versionen von PHP als veraltet gelten AL2, finden Sie in. Liste der Amazon Linux 2-Extras

Migration aus PHP 7.x-Versionen

Die PHP Upstream-Community hat eine umfassende Migrationsdokumentation für die Umstellung von PHP 7.4 auf PHP 8.0 zusammengestellt. In Kombination mit der Dokumentation, auf die im vorherigen Abschnitt zur Migration auf PHP 8.1 und PHP 8.2 verwiesen wurde, stehen Ihnen alle Schritte zur Verfügung, die für die Migration Ihrer Basisanwendung PHP auf die moderne PHP Version erforderlich sind.

Das PHPProjekt führt eine Liste und einen Zeitplan der unterstützten Versionen sowie eine Liste der nicht unterstützten Branches.

> **Note**
>
> Als AL2 023 veröffentlicht wurde, PHPwurden alle 7.x- und 5.x-Versionen von von der PHPCommunity nicht unterstützt und waren nicht als Optionen in 023 enthalten. AL2

Pythonin AL2

AL2 bietet Support und Sicherheitspatches für Python 2.7 bis Juni 2026 als Teil unseres langfristigen Supports für AL2 Kernpakete. Diese Unterstützung geht über die vorherige Python Community-Erklärung von Python 2.7 EOL vom Januar 2020 hinaus.

> **Note**
>
> AL2023 hat 2.7 vollständig entfernt. Python Alle Komponenten, die dies erfordern, Python sind jetzt so geschrieben, dass sie mit Python 3 funktionieren.

AL2 verwendet den `yum` Paketmanager, der stark von Python 2.7 abhängig ist. In AL2 Version 023 wurde der `dnf` Paketmanager auf Version Python 3 migriert und benötigt Python 2.7 nicht mehr. AL2023 wurde komplett auf 3 umgestellt. Python Wir empfehlen Ihnen, Ihre Migration auf Python 3 abzuschließen.

Einrosten AL2

Möglicherweise möchten Sie AL2 mithilfe einer mitgelieferten Toolchain Ihren eigenen Code erstellen, in Rustden geschrieben wurde. AL2

Die Rust Toolchain wird während der gesamten Lebensdauer von aktualisiert. AL2 Dies kann als Reaktion auf ein CVE in der von uns gelieferten Toolchain oder als Voraussetzung für ein CVE-Update in einem anderen Paket geschehen.

Rustist eine relativ schnelllebige Sprache, mit Neuerscheinungen in einem Rhythmus von etwa sechs Wochen. Die neuen Versionen könnten neue Sprach- oder Standardbibliotheksfunktionen hinzufügen. Zwar AL2 werden im Laufe der Laufzeit neue Versionen der Rust Toolchain integriert, dies wird jedoch nicht mit den Vorgängerversionen Schritt halten. Rust Daher ist die Verwendung der unter bereitgestellten Rust Toolchain AL2 möglicherweise nicht geeignet, wenn Sie Rust Code mit den neuesten Funktionen der Sprache erstellen möchten. Rust

Während der Lebensdauer von AL2 werden frühere Paketversionen nicht aus den Repositorys entfernt. Wenn eine frühere Rust Toolchain erforderlich ist, können Sie auf Fehler- und Sicherheitskorrekturen neuerer Rust Toolchains verzichten und eine frühere Version aus den Repositorys mit den gleichen Prozessen installieren, die für jedes RPM verfügbar sind.

Um Ihren eigenen Rust Code zu erstellen AL2, verwenden Sie die mitgelieferte Rust Toolchain AL2 mit dem Wissen, dass diese Toolchain im Laufe der Lebensdauer von weiterentwickelt werden kann. AL2

AL2 Kernel

AL2 wurde ursprünglich mit einem 4.14-Kernel ausgeliefert, mit Version 5.10 als aktueller Standardversion. Wenn Sie immer noch einen 4.14-Kernel verwenden, sollten Sie auf den 5.10-Kernel migrieren.

Kernel-Live-Patching wird auf unterstützt. AL2

Themen

AL2 unterstützte Kernel

Unterstützte Kernel-Versionen

Derzeit AL2 AMIs sind sie mit den Kernel-Versionen 4.14 und 5.10 verfügbar, wobei Version 5.10 die Standardversion ist. Wir empfehlen, ein AL2 AMI mit Kernel 5.10 zu verwenden.

AL2023 AMIs sind mit der Kernel-Version 6.1 verfügbar. Weitere Informationen finden Sie unter AL2023 Kernel changes von AL2 im Amazon Linux 2023 User Guide.

Support-Zeitrahmen

Der 5.10-Kernel, auf dem verfügbar ist, AL2 wird unterstützt, bis das AL2 AMI das Ende der Standardunterstützung erreicht.

Live-Patch-Support

AL2 Kernel-Version	Kernel-Live-Patching wird unterstützt
4.14	Ja
5,10	Ja
5,15	Nein

Kernel Live Patching aktiviert AL2

> **Important**
>
> Amazon Linux wird das Live-Patchen für AL2 Kernel 4.14 am 31.10.2025 beenden. Kunden wird empfohlen, Kernel 5.10 als Standardkernel für zu verwenden AL2 (siehe AL2 unterstützte Kernel) oder mit den Kerneln 6.1 und 6.12 auf Version 023 AL2 umzusteigen. Amazon Linux wird Live-Patches für AL2 Kernel 5.10 bis zum Ende der Lebensdauer AL2 am 30.06.2026 bereitstellen.

Kernel Live Patching for AL2 ermöglicht es Ihnen, spezifische Sicherheitslücken und kritische Bug-Patches auf einen laufenden Linux-Kernel anzuwenden, ohne Neustarts oder Unterbrechungen laufender Anwendungen. Auf diese Weise können Sie von einer verbesserten Service- und Anwendungsverfügbarkeit profitieren und gleichzeitig diese Korrekturen anwenden, bis das System neu gestartet werden kann.

Informationen zu Kernel Live Patching für AL2 023 finden Sie unter Kernel Live Patching on AL2 023 im Amazon Linux 2023 User Guide.

AWS veröffentlicht zwei Arten von Kernel-Live-Patches für: AL2

- Sicherheitsupdates – Enthält Updates für die häufigsten Schwachstellen und Risiken von Linux (Common Vulnerabilities and Exposures, CVE). Diese Updates werden typischerweise als wichtig oder kritisch eingestuft, wobei die Amazon Linux Security Advisory-Bewertungen verwendet werden. Sie entsprechen im Allgemeinen einem CVSS-Score (Common Vulnerability Scoring System) von 7 und höher. In einigen Fällen AWS kann es Updates bereitstellen, bevor ein CVE zugewiesen wird. In diesen Fällen erscheinen die Patches möglicherweise als Bugfixes.
- Fehlerkorrekturen — Beinhaltet Korrekturen für kritische Fehler und Stabilitätsprobleme, die nicht damit CVEs in Zusammenhang stehen.

AWS bietet Kernel-Live-Patches für eine AL2 Kernel-Version für bis zu 3 Monate nach ihrer Veröffentlichung. Nach Ablauf der dreimonatigen Frist müssen Sie auf eine spätere Kernel-Version aktualisieren, um weiterhin Live-Kernel-Patches zu erhalten.

AL2 Kernel-Live-Patches werden als signierte RPM-Pakete in den vorhandenen AL2 Repositorys zur Verfügung gestellt. Die Patches können mithilfe vorhandener Yum-Workflows auf einzelnen Instanzen

installiert werden, oder sie können mithilfe von AWS Systems Manager auf einer Gruppe verwalteter Instanzen installiert werden.

Kernel Live Patching on AL2 wird ohne zusätzliche Kosten zur Verfügung gestellt.

Themen

Unterstützte Konfigurationen und Voraussetzungen

Kernel Live Patching wird auf EC2 Amazon-Instances und lokalen virtuellen Maschinen unterstützt. AL2

Um Kernel Live Patching auf zu verwenden AL2, müssen Sie Folgendes verwenden:

- Kernel-Version `4.14` oder `5.10` auf der `x86_64`-Architektur
- Kernel-Version `5.10` auf der `ARM64`-Architektur

Richtlinienanforderungen

Um Pakete aus Amazon Linux-Repositorys herunterzuladen, EC2 benötigt Amazon Zugriff auf serviceeigene Amazon S3 S3-Buckets. Wenn Sie in Ihrer Umgebung einen Amazon Virtual Private Cloud (VPC)-Endpunkt für Amazon S3 verwenden, müssen Sie sicherstellen, dass Ihre VPC-Endpunktrichtlinie den Zugriff auf diese öffentlichen Buckets zulässt.

In der Tabelle werden die einzelnen Amazon S3 S3-Buckets beschrieben, auf die EC2 möglicherweise für Kernel Live Patching zugegriffen werden muss.

S3 Bucket-ARN	Description
arn:aws:s3: ::packages. *region*.amazonaws.com/*	Amazon-S3-Bucket mit Amazon-Linux-AMI-Paketen
arn:aws:s3: ::repo. *region*.amazonaws.com/*	Amazon-S3-Bucket mit Amazon-Linux-AMI-Repositories

S3 Bucket-ARN	Description
arn:aws:s3: ::amazonlinux. *region*.amazonaws.com/*	Amazon S3 S3-Bucket mit AL2 Repositorys
arn:aws:s3: ::amazonlinux-2-repos- /* *region*	Amazon S3 S3-Bucket mit AL2 Repositorys

Die folgende Richtlinie veranschaulicht, wie Sie den Zugriff auf Identitäten und Ressourcen einschränken, die Ihrer Organisation gehören, und Zugriff auf die Amazon-S3-Buckets gewähren, die für Kernel-Live-Patching erforderlich sind. Ersetzen Sie *region* *principal-org-id* und *resource-org-id* durch die Werte Ihrer Organisation.

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/*"
      ]
    }
  ]
}
```

Arbeiten mit Kernel-Live-Patching

Sie können Kernel Live Patching auf einzelnen Instances über die Befehlszeile auf der Instance selbst aktivieren und verwenden, oder Sie können Kernel Live Patching mit AWS Systems Manager für eine Gruppe verwalteter Instanzen aktivieren und verwenden.

In den folgenden Abschnitten wird erläutert, wie Sie Kernel-Live-Patching auf einzelnen Instances über die Befehlszeile aktivieren und verwenden.

Weitere Informationen zur Aktivierung und Verwendung von Kernel Live Patching für eine Gruppe verwalteter Instanzen finden Sie unter Verwenden von Kernel Live Patching auf AL2 Instanzen im Benutzerhandbuch.AWS Systems Manager

Themen

- Aktivieren des Kernel-Live-Patching
- Anzeigen der verfügbaren Kernel-Live-Patches
- Anwenden von Kernel-Live-Patches
- Anzeigen der angewendeten Kernel-Live-Patches
- Deaktivieren des Kernel-Live-Patching

Aktivieren des Kernel-Live-Patching

Kernel Live Patching ist standardmäßig deaktiviert. AL2 Um Live-Patching zu verwenden, müssen Sie das yum-Plugin für Kernel-Live-Patching installieren und die Live-Patching-Funktionalität aktivieren.

Voraussetzungen

Kernel-Live-Patching erfordert `binutils`. Wenn Sie `binutils` nicht installiert haben, installieren Sie es mit dem folgenden Befehl:

```
$ sudo yum install binutils
```

So aktivieren Sie das Kernel-Live-Patching:

1. Kernel-Live-Patches sind für die folgenden AL2 Kernel-Versionen verfügbar:

   - Kernel-Version `4.14` oder `5.10` auf der `x86_64`-Architektur
   - Kernel-Version `5.10` auf der `ARM64`-Architektur

   Um Ihre Kernel-Version zu überprüfen, führen Sie den folgenden Befehl aus.

   ```
   $ sudo yum list kernel
   ```

2. Wenn Sie bereits eine unterstützte Kernel-Version haben, überspringen Sie diesen Schritt. Wenn Sie keine unterstützte Kernel-Version haben, führen Sie die folgenden Befehle aus, um den Kernel auf die neueste Version zu aktualisieren und die Instance neu zu starten.

   ```
   $ sudo yum install -y kernel
   ```

   ```
   $ sudo reboot
   ```

3. Installieren Sie das yum-Plugin für Kernel-Live-Patching.

   ```
   $ sudo yum install -y yum-plugin-kernel-livepatch
   ```

4. Aktivieren Sie das yum-Plugin für Kernel-Live-Patching.

   ```
   $ sudo yum kernel-livepatch enable -y
   ```

   Mit diesem Befehl wird auch die neueste Version des Kernel-Live-Patch-RPM aus den konfigurierten Repositorys installiert.

5. Um zu überprüfen, ob das yum-Plugin für das Kernel-Live-Patching erfolgreich installiert wurde, führen Sie den folgenden Befehl aus.

```
$ rpm -qa | grep kernel-livepatch
```

Wenn Sie Kernel-Live-Patching aktivieren, wird automatisch ein leeres Kernel-Live-Patch-RPM angewendet. Wenn Kernel-Live-Patching erfolgreich aktiviert wurde, gibt dieser Befehl eine Liste zurück, die das anfänglich leere Kernel-Live-Patch-RPM enthält. Es folgt eine Beispielausgabe.

```
yum-plugin-kernel-livepatch-1.0-0.11.amzn2.noarch
kernel-livepatch-5.10.102-99.473-1.0-0.amzn2.x86_64
```

6. Installieren Sie das kpatch-Paket.

```
$ sudo yum install -y kpatch-runtime
```

7. Aktualisieren Sie den kpatch-Service, falls er zuvor installiert wurde.

```
$ sudo yum update kpatch-runtime
```

8. Starten Sie den kpatch-Service. Dieser Service lädt alle Live-Patches des Kernels bei der Initialisierung oder beim Booten.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

9. Aktivieren Sie das Thema Kernel Live Patching in der AL2 Extras-Bibliothek. Dieses Thema enthält die Kernel-Live-Patches.

```
$ sudo amazon-linux-extras enable livepatch
```

Anzeigen der verfügbaren Kernel-Live-Patches

Amazon Linux-Sicherheitswarnungen werden über das Amazon Linux-Sicherheitszentrum veröffentlich. Weitere Informationen zu den AL2 Sicherheitswarnungen, zu denen auch Warnungen für Kernel-Live-Patches gehören, finden Sie im Amazon Linux Security Center. Kernel-Live-Patches wird das Präfix `ALASLIVEPATCH` vorangestellt. Das Amazon Linux-Sicherheitszentrum listet möglicherweise keine Live-Kernel-Patches auf, die Fehler beheben.

Sie können sich auch die verfügbaren Kernel-Live-Patches ansehen, um Hinweise zu erhalten und die Befehlszeile zu CVEs verwenden.

So listen Sie alle verfügbaren Kernel-Live-Patches für Advisories auf:

Verwenden Sie den folgenden Befehl.

```
$ yum updateinfo list
```

Das folgende Beispiel zeigt eine Ausgabe.

```
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
```

Um alle verfügbaren Kernel-Live-Patches aufzulisten für CVEs

Verwenden Sie den folgenden Befehl.

```
$ yum updateinfo list cves
```

Das folgende Beispiel zeigt eine Ausgabe.

```
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
```

Anwenden von Kernel-Live-Patches

Sie wenden Kernel-Live-Patches unter Verwendung des yum-Paketmanagers auf dieselbe Weise an, wie Sie regelmäßige Updates anwenden würden. Das Yum-Plugin für Kernel Live Patching verwaltet die Kernel-Live-Patches, die angewendet werden können.

> **Tip**
>
> Wir empfehlen Ihnen, Ihren Kernel regelmäßig mit Kernel Live Patching zu aktualisieren, um sicherzustellen, dass er bestimmte wichtige und kritische Sicherheitsfixes erhält, bis das System neu gestartet werden kann. Bitte überprüfen Sie auch, ob zusätzliche Fixes für das

native Kernel-Paket verfügbar gemacht wurden, die nicht als Live-Patches bereitgestellt werden können, und führen Sie in diesen Fällen ein Update durch und starten Sie das Kernel-Update neu.

Sie können wählen, ob Sie einen bestimmten Kernel-Live-Patch oder alle verfügbaren Kernel-Live-Patches zusammen mit Ihren regelmäßigen Sicherheitsupdates anwenden wollen.

So wenden Sie einen bestimmten Kernel-Live-Patch an:

1. Holen Sie sich die Kernel-Live-Patch-Version mit einem der in Anzeigen der verfügbaren Kernel-Live-Patches beschriebenen Befehle.
2. Wenden Sie den Kernel-Live-Patch für Ihren AL2 Kernel an.

   ```
   $ sudo yum install kernel-livepatch-kernel_version.x86_64
   ```

   Der folgende Befehl wendet beispielsweise einen Kernel-Live-Patch für die AL2 -Kernel-Version `5.10.102-99.473` an.

   ```
   $ sudo yum install kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
   ```

So wenden Sie alle verfügbaren Kernel-Live-Patches zusammen mit Ihren regelmäßigen Sicherheitsupdates an:

Verwenden Sie den folgenden Befehl.

```
$ sudo yum update --security
```

Lassen Sie die Option `--security` weg, um Bugfixes einzuschließen.

Important

- Die Kernel-Version wird nach der Anwendung von Kernel-Live-Patches nicht aktualisiert. Die Version wird erst nach einem Neustart der Instance auf die neue Version aktualisiert.
- Ein AL2 Kernel erhält Kernel-Live-Patches für einen Zeitraum von drei Monaten. Nach Ablauf der dreimonatigen Frist werden für diese Kernel-Version keine neuen Kernel-Live-Patches mehr veröffentlicht. Um nach Ablauf der dreimonatigen Frist weiterhin Kernel-Live-

Patches zu erhalten, müssen Sie die Instance neu starten, um auf die neue Kernel-Version zu wechseln, die dann die nächsten drei Monate lang weiterhin Kernel-Live-Patches erhält. Um das Support-Fenster für Ihre Kernel-Version zu überprüfen, führen Sie `yum kernel-livepatch supported` aus.

Anzeigen der angewendeten Kernel-Live-Patches

So zeigen Sie die angewendeten Kernel-Live-Patches an:

Verwenden Sie den folgenden Befehl.

```
$ kpatch list
```

Der Befehl gibt eine Liste der geladenen und installierten Sicherheitsupdate-Kernel-Live-Patches zurück. Es folgt eine Beispielausgabe.

```
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

Ein einziger Kernel-Live-Patch kann mehrere Live-Patches enthalten und installieren.

Deaktivieren des Kernel-Live-Patching

Wenn Sie das Kernel-Live-Patching nicht mehr verwenden möchten, können Sie es jederzeit deaktivieren.

So deaktivieren Sie das Kernel-Live-Patching:

1. Entfernen Sie die RPM-Pakete für die angewandten Kernel-Live-Patches.

```
$ sudo yum kernel-livepatch disable
```

2. Deinstallieren Sie das yum-Plugin für Kernel-Live-Patching.

```
$ sudo yum remove yum-plugin-kernel-livepatch
```

3. Starten Sie die Instance neu.

```
$ sudo reboot
```

Einschränkungen

Kernel-Live-Patching hat die folgenden Einschränkungen:

- Beim Anwenden eines Kernel-Live-Patches können Sie keinen Ruhezustand ausführen, erweiterte Debugging-Tools (wie SystemTap kprobes und EBPF-basierte Tools) verwenden oder auf ftrace-Ausgabedateien zugreifen, die von der Kernel Live Patching-Infrastruktur verwendet werden.
-

> **Note**
>
> Aufgrund technischer Einschränkungen können einige Probleme nicht mit Live-Patching behoben werden. Aus diesem Grund werden diese Fixes nicht im Kernel-Live-Patch-Paket, sondern nur im nativen Kernel-Paket-Update mitgeliefert. Sie können das native Kernel-Paket-Update installieren und das System neu starten, um die Patches wie gewohnt zu aktivieren.

Häufig gestellte Fragen

Häufig gestellte Fragen zu Kernel Live Patching für AL2 finden Sie in den häufig gestellten Fragen zu Amazon Linux 2 Kernel Live Patching.

AL2 Extras-Bibliothek

> **Warning**
>
> Das `epel` Extra aktiviert das EPEL7 Repository eines Drittanbieters. Ab dem 30.06.2024 wird das EPEL7 Drittanbieter-Repository nicht mehr verwaltet.
> Dieses Drittanbieter-Repository wird keine future Updates enthalten. Das bedeutet, dass es keine Sicherheitskorrekturen für Pakete im EPEL-Repository geben wird.
> Optionen für einige EPEL Pakete finden Sie im EPEL Abschnitt des Amazon Linux 2023-Benutzerhandbuchs.

Mit können Sie die Extras-Bibliothek verwenden AL2, um Anwendungs- und Softwareupdates auf Ihren Instances zu installieren. Dieses Software-Updates werden als Themen bezeichnet. Sie können eine bestimmte Version eines Themas installieren oder die Versionsinformationen weglassen, um die neueste Version zu verwenden. Extras tragen dazu bei, dass Sie keine Kompromisse zwischen der Stabilität eines Betriebssystems und der Aktualität der verfügbaren Software eingehen müssen.

Der Inhalt der Extras-Themen ist von der Amazon Linux-Richtlinie zu langfristigem Support und Binärkompatibilität ausgenommen. Extras-Themen bieten Zugriff auf eine kuratierte Liste von Paketen. Die Versionen der Pakete werden möglicherweise häufig aktualisiert oder werden möglicherweise nicht für den gleichen Zeitraum unterstützt wie AL2.

> **Note**
>
> Einzelne Extras-Themen sind möglicherweise veraltet, bevor EOL AL2 erreicht wird.

Verwenden Sie den folgenden Befehl, um die verfügbaren Themen aufzulisten.

```
[ec2-user ~]$ amazon-linux-extras list
```

Verwenden Sie den folgenden Befehl, um ein Thema zu aktivieren und die neueste Version des zugehörigen Pakets zu installieren, um die Aktualität sicherzustellen.

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

Verwenden Sie den folgenden Befehl, um Themen zu aktivieren und bestimmte Versionen ihrer Pakete zu installieren, um die Stabilität zu gewährleisten.

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

Verwenden Sie den folgenden Befehl, um ein aus einem Thema installiertes Paket zu entfernen.

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk
 '{ print $1 }')
```

> **Note**
>
> Mit diesem Befehl werden keine Pakete entfernt, die als Abhängigkeiten des Extra installiert wurden.

Um ein Thema zu deaktivieren und die Pakete für den Yum-Paketmanager unzugänglich zu machen, verwenden Sie den folgenden Befehl.

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

> **Important**
>
> Dieser Befehl ist für fortgeschrittene Benutzer gedacht. Eine unsachgemäße Verwendung dieses Befehls kann zu Paketkompatibilitätskonflikten führen.

Liste der Amazon Linux 2-Extras

Zusätzlicher Name	Veraltetes Datum
BCC	
GraphicsMagick1.3	
R3,4	
R4	

Zusätzlicher Name	Veraltetes Datum
ansible 2	2023-09-30
aws-nitro-enclaves-cli	
als CLI 1	
collectd	
d-python3 gesammelt	
corretto8	
dnsmasq	
dnsmasq 2,85	01.05.2025
Docker	
ecs	
Emacs	14.11.2018
abstoßen	30.06.2024
Feuerwerkskörper	08.11.2022
Firefox	
Gimp	14.11.2018
Golang 1.11	2023-08-01
Golang 1,19	2023-09-30
Golang 1,9	2018-12-14
Haproxy 2	
httpd_module	

Zusätzlicher Name	Veraltetes Datum
java-openjdk11	30.09.2024
Kernel-5.10	
Kernel-5.15	
Kernel-5.4	
kernel-ng	08.08.2022
Lampe-Mariadb10.2-php7.2	30.11.2020
Libreoffice	
Live-Patch	
Glanz	
Glanz 2.10	
lynis	
Mariadb10.5	24.06.2025
mate-desktop1.x	
memcached 1.5	
verspotten	
verspotten 2	
mono	
nano	14.11.2018
Ngin x 1	
nginx 1.12	20.09.2019

Zusätzlicher Name	Veraltetes Datum
Nginx 1.22.1	
PHP 7.1	15.01.2020
PHP 7,2	30.11.2020
PHP 7,3	06.12.2021
PHP 7,4	03.11.2022
PHP8,0	26.11.2023
PHP 8,1	31.12.2025
PHP 8,2	
postgresql10	30.09.2023
postgresql11	09.11.2023-
postgresql12	2024-11-14
postgresql13	13.11.2025
postgresql-14	
PostgreSQL 9.6	09.08.2022
python3	22.08.2018
python3.8	2024-10-14
Rot ist 4,0	25.05.2021
redis6	2026-01-31
Rubin 2.4	27.08.2020
Rubin 2.6	2023-03-31

Zusätzlicher Name	Veraltetes Datum
Rubin 3.0	2024-03-31
rosten 1	01.05.2025
Selinux-ng	
Tintenfisch 4	30.09.2023
Testen	
Tomcat 8.5	2024-03-31
Tomcat 9	
ungebunden1.13	01.05.2025
ungebunden1,17	
vim	14.11.2018

AL2 Reservierte Benutzer und Gruppen

AL2 weist bestimmten Benutzern und Gruppen sowohl bei der Bereitstellung des Images als auch bei der Installation bestimmter Pakete vorab zu. Die Benutzer, Gruppen und die ihnen UIDs zugewiesenen Benutzer GIDs sind hier aufgeführt, um Konflikte zu vermeiden.

Themen

Liste der reservierten Amazon Linux 2-Benutzer

Aufgeführt nach UID

Benutzername	Benutzerkennung (UID)
Root	0
bin	1
deamon	2
adm	3
lp	4
sync	5
shutdown	6
Anhalten	7
Post	8
uucp	10
operator	11
Spiele	12

Benutzername	Benutzerkennung (UID)
ftp	14
Profil	16
Impulsgeber	17
Tintenfisch	23
genannt	25
postgres	26
mysql-	27
nscd	28
nscd	28
Rpcuser	29
rpc	32
Ein Mann und ein Backup	33
ntp	38
Postbote	41
gdm	42
mailnull	47
Apache	48
smmsp	51
Tomcat	53
ldap	55

Benutzername	Benutzerkennung (UID)
tss	59
nslcd	65
Pegasus	66
Avahi	70
tcpdump	72
sshd	74
radvd	75
Cyrus	76
Armbanduhr	77
fax	78
dbus	81
postfix	89
Quagga	92
im Radius	95
im Radius	95
hsqldb	96
Taubenbett	97
Ident	98
niemand	99
Qemu	107

Benutzername	Benutzerkennung (UID)
usbmuxd	113
stap-Server	155
Avahi-AutoIPD	170
Impuls	171
RTKIT	172
dhcpd	177
Sanlock	179
haproxy	188
Hacluster	189
systemd-journal-gateway	191
systemd-Netzwerk	192
systemd-resolve	193
uuidd	357
Tang	358
stapdev	359
Stapsys	360
Stapus	361
systemd-journal-upload	362
systemd-journal-remote	363
geschliffen	364

Benutzername	Benutzerkennung (UID)
entwerfen	365
pcpqa	366
pcp	367
memcached	368
Ipsilon	369
ipaapi	370
KDC-Proxy	371
Götter	372
sssd	373
Gluster	374
Fehden	375
Taubenull	376
koroqnet	377
Gabelkopf	378
Muschelscan	379
beansprucht	380
Clamupdate	381
Farben	382
Geoclue	383
aws-kinesis-agent-user	384

Benutzername	Benutzerkennung (UID)
C-Agent	385
ungebunden	386
höflich	387
Saslauth	388
dirsrv	389
chrony	996
ec2-instance-connect	997
rngd	998
libstoragemgmt	999
ec2-Benutzer	1000
nfs niemand	65534

Nach Namen gelistet

Benutzername	Benutzerkennung (UID)
adm	3
Ein Mann und ein Backup	33
Apache	48
Armbanduhr	77
Avahi	70
Avahi-AutoIPD	170

Benutzername	Benutzerkennung (UID)
aws-kinesis-agent-user	384
bin	1
chrony	996
beansprucht	380
Clamscan	379
klammer aktualisieren	381
Gabelkopf	378
Farben	382
koroqnet	377
Kagenz	385
Cyrus	76
deamon	2
dbus	81
dhcpd	177
dirsrv	389
Taubenbett	97
Taubenull	376
ec2-instance-connect	997
ec2-Benutzer	1000
fax	78

Benutzername	Benutzerkennung (UID)
Lefts	375
ftp	14
Spiele	12
gdm	42
Geoclue	383
Gluster	374
Hacluster	189
Anhalten	7
haproxy	188
hsqldb	96
Ident	98
ipaapi	370
Ipsilon	369
KDC-Proxy	371
ldap	55
libstoragemgmt	999
lp	4
Post	8
Postbote	41
mailnull	47

Benutzername	Benutzerkennung (UID)
memcached	368
mysql-	27
genannt	25
NFS Niemand	65534
niemand	99
nscd	28
nscd	28
nslcd	65
ntp	38
Quoten	372
operator	11
Profil	16
pcp	367
pcpqa	366
Pegasus	66
entwerfen	365
Pikuser	17
höflich	387
postfix	89
postgres	26

Benutzername	Benutzerkennung (UID)
Impuls	171
Qemu	107
Quagga	92
im Radius	95
im Radius	95
radvd	75
rngd	998
Root	0
rpc	32
RPC-Benutzer	29
rtkit	172
geschliffen	364
Sanlock	179
Saslauth	388
shutdown	6
smmsp	51
Tintenfisch	23
sshd	74
sssd	373
stap-Server	155

Benutzername	Benutzerkennung (UID)
stapdev	359
Stapsys	360
Stapus	361
sync	5
systemd-journal-gateway	191
systemd-journal-remote	363
systemd-journal-upload	362
systemd-Netzwerk	192
systemd-resolve	193
Tang	358
tcpdump	72
Tomcat	53
tss	59
ungebunden	386
usbmuxd	113
uucp	10
uuidd	357

Liste der reservierten Gruppen von Amazon Linux 2

Von GID gelistet

Gruppenname	GID
Root	0
bin	1
deamon	2
sys	3
adm	4
TTY	5
Datenträger	6
Datenträger	6
lp	7
mem	8
Kem	9
Rad	10
CD-ROM	11
Post	12
uucp	14
man	15
Profil	16
Impulsgeber	17
wählen	18
Diskette	19

Gruppenname	GID
Spiele	20
slokieren	21
utmp	22
Tintenfisch	23
genannt	25
postgres	26
mysql-	27
nscd	28
nscd	28
Rpcuser	29
rpc	32
Band	33
Band	33
Verlockung	35
kvm	36
ntp	38
video	39
eintauchen	40
Postbote	41
gdm	42

Gruppenname	GID
mailnull	47
Apache	48
ftp	50
smmsp	51
Tomcat	53
Verriegelung	54
ldap	55
tss	59
audio	63
Pegasus	65
Avahi	70
tcpdump	72
sshd	74
radvd	75
Saslauth	76
Saslauth	76
Armbanduhr	77
fax	78
dbus	81
screen	84

Gruppenname	GID
Quaggavt	85
wbpriv	88
wbpriv	88
postfix	89
Postdrop	90
Quagga	92
im Radius	95
im Radius	95
hsqldb	96
Taubenbett	97
Ident	98
niemand	99
users	100
Qemu	107
usbmuxd	113
stap-Server	155
Stapus	156
Stapus	156
Stapsys	157
stapdev	158

Gruppenname	GID
Avahi-AutoIPD	170
Impuls	171
RT-Kit	172
dhcpd	177
Sanlock	179
haproxy	188
hat einen Kunden	189
systemd-journal	190
systemd-journal	190
systemd-journal-gateway	191
systemd-Netzwerk	192
systemd-resolve	193
beschwören	351
Drahthaie	352
uuidd	353
Tang	354
systemd-journal-upload	355
sfcb	356
systemd-journal-remote	356
geschliffen	357

Gruppenname	GID
entwerfen	358
pcpqa	359
pcp	360
memcached	361
virtuelles Einloggen	362
Ipsilon	363
Stck. 11	364
ipaapi	365
KDC-Proxy	366
Quoten	367
sssd	368
Libvirt	369
Gluster	370
Fehden	371
Taubenull	372
Docker	373
koroqnet	374
Gabelkopf	375
Muschelscan	376
beansprucht	377

Gruppenname	GID
Virengruppe	378
Virusgruppe	378
Virusgruppe	378
Klammer aktualisieren	379
Farben	380
Geoclue	381
admin drucken	382
aws-kinesis-agent-user	383
C-Agent	384
Puls-RT	385
Pulszugriff	386
ungebunden	387
höflich	388
dirsrv	389
cgred	993
chrony	994
ec2-instance-connect	995
rngd	996
libstoragemgmt	997
SSH-Schlüssel	998

Gruppenname	GID
input	999
ec2-Benutzer	1000
nfs niemand	65534

Nach Namen gelistet

Gruppenname	GID
adm	4
Apache	48
Armbanduhr	77
audio	63
Avahi	70
Avahi-AutoIPD	170
aws-kinesis-agent-user	383
bin	1
CD-ROM	11
cgred	993
chrony	994
beansprucht	377
Muschelscan	376
Klammer aktualisieren	379

Gruppenname	GID
Gabelkopf	375
Farben	380
koroqnetd	374
C-Agent	384
deamon	2
dbus	81
dhcpd	177
wählen	18
eintauchen	40
dirsrv	389
Datenträger	6
Datenträger	6
Docker	373
Taubenbett	97
Taubenull	372
ec2-instance-connect	995
ec2-Benutzer	1000
fax	78
Lefts	371
Diskette	19

Gruppenname	GID
ftp	50
Spiele	20
gdm	42
Geoclue	381
Gluster	370
hat einen Kunden	189
haproxy	188
hsqldb	96
Ident	98
input	999
ipaapi	365
Ipsilon	363
kdc-Proxy	366
kmem	9
kvm	36
ldap	55
libstoragemgmt	997
Libvirt	369
Verriegelung	54
lp	7

Gruppenname	GID
Post	12
Postbote	41
mailnull	47
man	15
mem	8
memcached	361
mysql-	27
genannt	25
NFS Niemand	65534
niemand	99
nscd	28
nscd	28
ntp	38
Quoten	367
profil	16
pcp	360
pcpqa	359
Pegasus	65
entwerfen	358
Stck. 11	364

Gruppenname	GID
Pikuser	17
höflich	388
Postdrop	90
postfix	89
postgres	26
admin drucken	382
Impuls	171
Puls-Zugriff	386
Puls-RT	385
Qemu	107
Quagga	92
Quaggavt	85
im Radius	95
im Radius	95
radvd	75
rngd	996
Root	0
rpc	32
RPC-Benutzer	29
rtkit	172

Gruppenname	GID
geschliffen	357
Sanlock	179
Saslauth	76
Saslauth	76
screen	84
sfcb	356
slokieren	21
smmsp	51
Tintenfisch	23
ssh_keys	998
sshd	74
sssd	368
stap-Server	155
stapdev	158
Stapsys	157
Stapus	156
Stapus	156
sagt	3
systemd-journal	190
systemd-journal	190

Gruppenname	GID
systemd-journal-gateway	191
systemd-journal-remote	356
systemd-journal-upload	355
systemd-Netzwerk	192
systemd-resolve	193
Tang	354
Band	33
Band	33
tcpdump	72
Tomcat	53
tss	59
TTY	5
ungebunden	387
beschwören	351
usbmuxd	113
users	100
Versuchung	35
utmp	22
uucp	14
uuidd	353

Gruppenname	GID
video	39
virtuelles Einloggen	362
Virengruppe	378
Virusgruppe	378
Virusgruppe	378
wbpriv	88
wbpriv	88
Rad	10
Wireshark	352

AL2 Quellpakete

Sie können den Quellcode der in Ihrer Instance installierten Pakete zu Referenzzwecken anzeigen, indem sie die in Amazon Linux bereitgestellten Tools verwenden. Quellcodepakete sind für alle in Amazon Linux und in den Online-Paket-Repositorys enthaltenen Pakete verfügbar. Ermitteln Sie den Paketnamen für das Quellpaket, das Sie installieren möchten, und verwenden Sie den yumdownloader --source Befehl, um den Quellcode in Ihrer laufenden Instanz anzuzeigen. Beispiel:

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

Das Quell-RPM kann entpackt werden, und als Referenz können Sie sich den Quellbaum mit Standard-RPM-Tools ansehen. Wenn Sie das Debugging beendet haben, können Sie das Paket verwenden.

Sicherheit und Compliance in AL2

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWSbietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AL2 023 gelten, finden Sie unter AWSServices im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud: Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

FIPS-Modus aktivieren AL2

In diesem Abschnitt wird erklärt, wie die Federal Information Processing Standards (FIPS) aktiviert werden. AL2 Weitere Informationen über FIPS finden Sie unter:

- Federal Information Processing Standard (FIPS)
- Einhaltung FAQs: Bundesstandards für die Informationsverarbeitung

Voraussetzungen

- Eine bestehende AL2 EC2 Amazon-Instance mit Internetzugang zum Herunterladen der erforderlichen Pakete. Weitere Informationen zum Starten einer AL2 EC2 Amazon-Instance finden Sie unterAL2 auf Amazon EC2.
- Sie müssen über SSH oder eine Verbindung zu Ihrer EC2 Amazon-Instance herstellenAWS Systems Manager.

> **Important**
>
> ED25519 SSH-Benutzerschlüssel werden im FIPS-Modus nicht unterstützt. Wenn Sie Ihre EC2 Amazon-Instance mit einem ED25519 SSH-Schlüsselpaar gestartet haben, müssen Sie mithilfe eines anderen Algorithmus (z. B. RSA) neue Schlüssel generieren. Andernfalls verlieren Sie möglicherweise den Zugriff auf Ihre Instance, nachdem Sie den FIPS-Modus aktiviert haben. Weitere Informationen finden Sie unter Schlüsselpaare erstellen im EC2 Amazon-Benutzerhandbuch.

Aktivieren des FIPS-Modus

1. Stellen Sie über SSH eine Connect zu Ihrer AL2 Instance her oderAWS Systems Manager.
2. Stellen Sie sicher, dass das System auf dem neuesten Stand ist. Weitere Informationen finden Sie unter Paket-Repository.
3. Installieren und aktivieren Sie das `dracut-fips` Modul, indem Sie die folgenden Befehle ausführen.

   ```
   sudo yum -y install dracut-fips
   sudo dracut -f
   ```

4. Aktivieren Sie den FIPS-Modus in der Linux-Kernel-Befehlszeile mit dem folgenden Befehl. Dadurch wird der FIPS-Modus systemweit für die in den FAQ aufgeführten Module aktiviert AL2

   ```
   sudo /sbin/grubby --update-kernel=ALL --args="fips=1"
   ```

5. Starten Sie Ihre Instance neu. AL2

   ```
   sudo reboot
   ```

6. Stellen Sie erneut eine Verbindung mit Ihrer Instance her und führen Sie den folgenden Befehl aus, um zu prüfen, ob der FIPS-Modus aktiviert ist.

   ```
   sysctl crypto.fips_enabled
   ```

   Die Ausgabe sollte folgendermaßen aussehen:

   ```
   crypto.fips_enabled = 1
   ```

Sie können auch überprüfen, ob OpenSSH im FIPS-Modus ist, indem Sie den folgenden Befehl ausführen:

```
ssh localhost 2>&1 | grep FIPS
```

Die Ausgabe sollte folgendermaßen aussehen:

```
FIPS mode initialized
```

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.