aws

Guida per l'utente

Amazon Linux 2

Amazon Linux 2: Guida per l’utente

Table of Contents

Cos'è Amazon Linux 2?

Amazon Linux 2 (AL2) è un sistema operativo Linux di Amazon Web Services (AWS). AL2 è progettato per fornire un ambiente stabile, sicuro e ad alte prestazioni per le applicazioni in esecuzione su Amazon EC2. Include anche pacchetti che consentono un'integrazione efficiente conAWS, tra cui strumenti di configurazione di avvio e molte AWS librerie e strumenti popolari. AWSfornisce aggiornamenti continui di sicurezza e manutenzione per tutte le istanze in esecuzione AL2. Molte applicazioni sviluppate su CentOS e distribuzioni simili vengono eseguite su. AL2 AL2 viene fornito senza costi aggiuntivi.

> **Note**
>
> AL2 non è più la versione corrente di Amazon Linux. AL2023 è il successore di. AL2 Per ulteriori informazioni, vedere Comparing AL2 and AL2 023 e l'elenco delle modifiche ai Package in AL2 023 nella 023 User AL2Guide.

> **Note**
>
> AL2 segue da vicino la versione originale di Firefox Extended Support Release (ESR) e si aggiorna alla prossima ESR non appena disponibile. Per ulteriori informazioni, consulta il calendario di rilascio di Firefox ESR e le note di rilascio di Firefox.

Disponibilità Amazon Linux

AWSfornisce AL2 023 e Amazon Linux 1 (AL1precedentemente Amazon Linux AMI). AL2 Se stai migrando da un'altra distribuzione Linux ad Amazon Linux, ti consigliamo di migrare a AL2 023.

> **Note**
>
> Il supporto standard per AL1 è terminato il 31 dicembre 2020. La fase AL1 di supporto alla manutenzione si è conclusa il 31 dicembre 2023. Per ulteriori informazioni su AL1 EOL e supporto di manutenzione, consulta il post del blog Update on Amazon Linux AMI end-of-life.

Per ulteriori informazioni su Amazon Linux, consulta AL2023 AL2, e AL1.

Per le immagini di container Amazon Linux, consulta Immagine di container Amazon Linux nella Guida per l'utente di Amazon Elastic Container Registry.

Funzionalità obsoleta in AL2

Le sezioni seguenti descrivono le funzionalità supportate AL2 e non presenti in. AL2023 Si tratta di funzionalità come caratteristiche e pacchetti che sono presenti in AL2, ma non in AL2023 e che non verranno aggiunte AL2023. Consulta la AL2 documentazione per sapere per quanto tempo questa funzionalità è supportata in AL2.

Pacchetti `compat-`

Tutti i pacchetti AL2 con il prefisso di `compat-` sono forniti per la compatibilità binaria con i vecchi binari che non sono ancora stati ricostruiti per le versioni moderne del pacchetto. Ogni nuova versione principale di Amazon Linux non includerà alcun `compat-` pacchetto delle versioni precedenti.

Tutti i `compat-` pacchetti in una versione di Amazon Linux (ad esempio AL2) non sono più disponibili e non sono presenti nella versione successiva (ad esempio AL2023). Consigliamo vivamente di ricostruire il software sulla base delle versioni aggiornate delle librerie.

Funzionalità obsoleta interrotta in, rimossa in AL1 AL2

Questa sezione descrive le funzionalità disponibili e non più disponibili in AL1. AL2

> **Note**
>
> Come parte della fase di supporto alla manutenzione di AL1, alcuni pacchetti avevano una data end-of-life (EOL) precedente alla fine di. AL1 Per ulteriori informazioni, vedere AL1 Package support statements.

> **Note**
>
> Alcune AL1 funzionalità sono state interrotte nelle versioni precedenti. Per informazioni, consulta le note AL1 di rilascio.

Argomenti

- x86 a 32 bit (i686) AMIs
- aws-apitools-*sostituito da AWS CLI
- systemdsostituisce in upstart AL2

x86 a 32 bit (i686) AMIs

Come parte della versione 2014.09 di, AL1 Amazon Linux ha annunciato che sarebbe stata l'ultima versione a produrre 32 bit. AMIs Pertanto, a partire dalla versione 2015.03 di, AL1 Amazon Linux non supporta più l'esecuzione del sistema in modalità a 32 bit. AL2 offre un supporto di runtime limitato per file binari a 32 bit su host x86-64 e non fornisce pacchetti di sviluppo per consentire la creazione di nuovi binari a 32 bit. AL2023 non include più pacchetti di spazio utente a 32 bit. Consigliamo agli utenti di completare la transizione al codice a 64 bit prima di migrare a 023. AL2

Se è necessario eseguire file binari a 32 bit su AL2 023, è possibile utilizzare lo spazio utente a 32 bit dall' AL2 interno di un AL2 contenitore eseguito su 023. AL2

`aws-apitools-*`sostituito da AWS CLI

Prima del rilascio di AWS CLI nel settembre 2013, AWS rendeva disponibile una serie di utilità da riga di comando, implementate inJava, che consentivano agli utenti di effettuare chiamate EC2 API Amazon. Questi strumenti sono stati interrotti nel 2015 e sono AWS CLI diventati il modo preferito per interagire con Amazon EC2 APIs dalla riga di comando. Il set di utilità da riga di comando include i seguenti `aws-apitools-*` pacchetti.

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

Il supporto upstream per i `aws-apitools-*` pacchetti è terminato a marzo 2017. Nonostante la mancanza di supporto upstream, Amazon Linux ha continuato a fornire alcune di queste utilità da riga di comando, ad esempio per fornire agli utenti `aws-apitools-ec2` la compatibilità con le versioni precedenti. AWS CLIÈ uno strumento più robusto e completo rispetto ai `aws-apitools-*` pacchetti in quanto viene mantenuto attivamente e fornisce un mezzo per utilizzarli tutti. AWS APIs

I `aws-apitools-*` pacchetti erano obsoleti a marzo 2017 e non riceveranno ulteriori aggiornamenti. Tutti gli utenti di uno di questi pacchetti devono migrare AWS CLI a. Questi pacchetti non sono presenti in AL2 023.

AL1 ha fornito anche `aws-apitools-rds` i pacchetti `aws-apitools-iam` and, che erano obsoleti e non sono più presenti in AL1 Amazon Linux da allora in poi. AL2

`systemd`sostituisce in **`upstart`** AL2

AL2 è stata la prima versione di Amazon Linux a utilizzare il sistema `systemd` init, `upstart` in AL1 sostituzione di. Qualsiasi configurazione `upstart` specifica deve essere modificata come parte della migrazione AL1 da una versione più recente di Amazon Linux. Non è possibile utilizzarlo `systemd` su AL1, quindi il passaggio da `upstart` a `systemd` può essere eseguito solo come parte del passaggio a una versione principale più recente di Amazon Linux come AL2 o AL2 023.

Funzionalità obsoleta e rimossa in AL2 AL2023

Questa sezione descrive le funzionalità disponibili e non più disponibili in AL2. AL2023

Argomenti

- Pacchetti x86 (i686) a 32 bit
- aws-apitools-*sostituito da AWS CLI
- awslogsobsoleto a favore dell'agente Amazon Logs unificato CloudWatch
- bzrsistema di controllo delle revisioni
- cgroup v1
- log4jhotpatch () log4j-cve-2021-44228-hotpatch
- lsb_release e il pacchetto system-lsb-core
- mcrypt
- OpenJDK (7) java-1.7.0-openjdk
- Python 2.7
- rsyslog-opensslsostituisce rsyslog-gnutls
- Servizio di informazione di rete (NIS)/yp
- Più nomi di dominio in Amazon VPC create-dhcp-options
- Sun RPC in glibc
- Impronta digitale della chiave OpenSSH nel registro audit

- ld.goldLinker
- ping6
- ftpPackage

Pacchetti x86 (i686) a 32 bit

Come parte della versione 2014.09 di AL1, abbiamo annunciato che sarebbe stata l'ultima versione a produrre 32 bit. AMIs Pertanto, a partire dalla versione 2015.03 di, AL1 Amazon Linux non supporta più l'esecuzione del sistema in modalità a 32 bit. AL2 fornisce un supporto di runtime limitato per file binari a 32 bit su host x86-64 e non fornisce pacchetti di sviluppo per consentire la creazione di nuovi binari a 32 bit. AL2023 non include più pacchetti di spazio utente a 32 bit. Consigliamo ai clienti di completare la transizione al codice a 64 bit.

Se è necessario eseguire file binari a 32 bit su AL2023, è possibile utilizzare lo spazio utente a 32 bit dall' AL2 interno di un AL2 contenitore in esecuzione su. AL2023

`aws-apitools-*`sostituito da AWS CLI

Prima del rilascio di settembre 2013, AWS rendeva disponibile una serie di utilità da riga di comando, implementate inJava, che consentivano ai clienti di effettuare chiamate API Amazon EC2. AWS CLI Questi strumenti sono stati dichiarati obsoleti nel 2015 e sono AWS CLI diventati il modo preferito per interagire con Amazon EC2 APIs dalla riga di comando. Ciò include i seguenti pacchetti. `aws-apitools-*`

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

Il supporto upstream per i `aws-apitools-*` pacchetti è terminato a marzo 2017. Nonostante la mancanza di supporto upstream, Amazon Linux ha continuato a fornire alcune di queste utilità da riga di comando (come`aws-apitools-ec2`) per fornire la retrocompatibilità ai clienti. AWS CLI È uno strumento più robusto e completo rispetto ai `aws-apitools-*` pacchetti in quanto viene mantenuto attivamente e fornisce un mezzo per utilizzarli tutti. AWS APIs

I `aws-apitools-*` pacchetti sono stati dichiarati obsoleti a marzo 2017 e non riceveranno ulteriori aggiornamenti. Tutti gli utenti di uno di questi pacchetti devono migrare AWS CLI a. Questi pacchetti non sono presenti in AL2023.

`awslogs`obsoleto a favore dell'agente Amazon Logs unificato CloudWatch

Il `awslogs`pacchetto è obsoleto AL2 e non è più presente in. AL2023 Viene sostituito dall'agente Unified CloudWatch Logs, disponibile nel pacchetto. `amazon-cloudwatch-agent` Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.

`bzr`sistema di controllo delle revisioni

Il sistema di controllo delle revisioni GNU Bazaar(`bzr`) è fuori produzione AL2 e non è più presente in. AL2023

Si consiglia agli utenti di `bzr` migrare i propri repository su. `git`

cgroup v1

AL2023 passa alla gerarchia dei gruppi di controllo unificati (cgroup v2), mentre utilizza cgroup v1. AL2 Poiché AL2 non supporta cgroup v2, questa migrazione deve essere completata come parte del passaggio a. AL2023

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

> **Note**
>
> Il `log4j-cve-2021-44228-hotpatch` pacchetto è obsoleto e rimosso in AL2 . AL2023

In risposta a CVE-2021-44228, Amazon Linux ha rilasciato una versione in pacchetto RPM di Hotpatch per Apache Log4j per e. AL1 AL2 Nell'annuncio dell'aggiunta dell'hotpatch ad Amazon Linux, abbiamo notato che «L'installazione dell'hotpatch non sostituisce l'aggiornamento a una versione log4j che mitiga CVE-2021-44228 o CVE-2021-45046».

L'hotpatch era una mitigazione per consentire il tempo necessario per applicare le patch `log4j`. La prima versione di disponibilità generale di risale a 15 mesi dopo CVE-2021-44228, quindi non viene fornita con l'hotpatch (abilitata o meno AL2023). AL2023

Si consiglia ai clienti che utilizzano le proprie versioni di `log4j` su Amazon Linux di assicurarsi di aver effettuato l'aggiornamento alle versioni non interessate da CVE-2021-44228 o CVE-2021-45046.

`lsb_release` e il pacchetto `system-lsb-core`

Storicamente, alcuni software richiamavano il `lsb_release` comando (fornito nel `system-lsb-core` pacchetto) AL2 per ottenere informazioni sulla distribuzione Linux su cui veniva eseguito. La Linux Standards Base (LSB) ha introdotto questo comando e le distribuzioni Linux lo hanno adottato. Le distribuzioni Linux si sono evolute per utilizzare lo standard più semplice per la memorizzazione di queste informazioni in `/etc/os-release` e altri file correlati.

Lo standard `os-release` viene da `systemd`. Per ulteriori informazioni, consulta la documentazione di systemd os-release.

AL2023 non viene fornito con il `lsb_release` comando e non include il `system-lsb-core` pacchetto. Il software deve completare la transizione allo standard `os-release` per mantenere la compatibilità con Amazon Linux e le altre principali distribuzioni Linux.

`mcrypt`

La `mcrypt` libreria e PHP l'estensione associata erano obsolete in AL2 e non sono più presenti in. AL2023

Upstream PHP ha reso obsoleta l'`mcrypt`estensione nella versione PHP 7.1, che è stata rilasciata per la prima volta a dicembre 2016 e ha avuto la sua versione finale a ottobre 2019.

L'ultima versione della `mcrypt` libreria upstream risale al 2007 e non ha effettuato la migrazione dal controllo di `cvs` revisione SourceForge richiesta per i nuovi commit nel 2017, con il commit più recente (e solo per i 3 anni precedenti) risalente al 2011, che rimuoveva la menzione che il progetto aveva un manutentore.

Si consiglia a tutti gli utenti `mcrypt` rimanenti di di trasferire il proprio codice suOpenSSL, poiché non `mcrypt` verrà aggiunto a. AL2023

OpenJDK (7) `java-1.7.0-openjdk`

> **Note**
>
> AL2023 fornisce diverse versioni di Amazon Corretto per supportare carichi di lavoro Java basati. I pacchetti OpenJDK 7 sono AL2 obsoleti in e non sono più presenti in. AL2023 Il JDK più vecchio disponibile AL2023 è fornito da Corretto 8.

Per ulteriori informazioni su Java su Amazon Linux, consultaJavanel AL2.

Python 2.7

> **Note**
>
> AL2023 Python 2.7 è stato rimosso, quindi tutti i componenti del sistema operativo che richiedono Python sono scritti per funzionare con Python 3. Per continuare a usare una versione di Python fornita e supportata da Amazon Linux, converti il codice di Python 2 in Python 3.

Per ulteriori informazioni su Python su Amazon Linux, consulta. Pythonnel AL2

`rsyslog-openssl`sostituisce `rsyslog-gnutls`

Il `rsyslog-gnutls` pacchetto è obsoleto in e non è più presente in AL2. AL2023 Il `rsyslog-openssl` pacchetto dovrebbe essere un sostituto immediato per qualsiasi utilizzo del pacchetto. `rsyslog-gnutls`

Servizio di informazione di rete (NIS)/`yp`

Il Network Information Service (NIS), originariamente chiamato Yellow Pages o YP è obsoleto e non è più presente in AL2. AL2023 Sono inclusi i seguenti pacchetti:`ypbind`,, `eypserv`. `yp-tools` Questa funzionalità è stata rimossa in altri pacchetti che si integrano con NIS AL2023.

Più nomi di dominio in Amazon VPC `create-dhcp-options`

In Amazon Linux 2, era possibile passare più nomi di dominio nel `domain-name` parametro a `create-dhcp-options`, il che avrebbe comportato `/etc/resolv.conf` qualcosa di

similesearch `foo.example.com bar.example.com`. Il DHCP server Amazon VPC invia l'elenco dei nomi di dominio forniti utilizzando DHCP l'opzione 15, che supporta solo un singolo nome di dominio (vedi RFC 2132 sezione 3.17). Poiché AL2023 viene utilizzato `systemd-networkd` per la configurazione di rete, che segue laRFC, questa funzionalità accidentale non è presente AL2 su AL2023

La AWS CLIdocumentazione di Amazon VPC dice quanto segue: «Alcuni sistemi operativi Linux accettano più nomi di dominio separati da spazi. Tuttavia, Windows e altri sistemi operativi Linux considerano il valore come un singolo dominio, il che si traduce in un comportamento imprevisto. Se il tuo set di DHCP opzioni è associato a un Amazon VPC con istanze che eseguono sistemi operativi che trattano il valore come un singolo dominio, specifica un solo nome di dominio. »

Su questi sistemi, ad esempio AL2023, se si specificano due domini utilizzando DHCP l'opzione 15 (che ne consente solo uno), e poiché lo spazio non è valido nei nomi di dominio, ciò comporterà la codifica del carattere di spazio come`032`, con conseguente contenitore. `/etc/resolv.conf search foo.exmple.com032bar.example.com`

Per supportare più nomi di dominio, un DHCP server deve utilizzare l'DHCPopzione 119 (vedere RFC 3397, sezione 2). Consulta la Amazon VPC User Guide per sapere quando questa funzionalità è supportata dal server Amazon VPC. DHCP

Sun RPC in **`glibc`**

L'implementazione di Sun RPC in `glibc` è obsoleta e rimossa in. AL2 AL2023 Si consiglia ai clienti di passare all'utilizzo della `libtirpc` libreria (disponibile in AL2 and AL2023) se sono necessarie Sun RPC funzionalità. L'adozione consente `libtirpc` inoltre alle applicazioni di supportareIPv6.

Questa modifica riflette la più ampia adozione da parte della comunità della `glibc` rimozione a monte di questa funzionalità, ad esempio la rimozione delle Sun RPC interfacce da Fedora e una modifica `glibc` simile in Gentoo.

Impronta digitale della chiave OpenSSH nel registro **`audit`**

Più avanti nel ciclo di vita di AL2, è stata aggiunta una patch al pacchetto OpenSSH per emettere l'impronta digitale della chiave utilizzata per l'autenticazione. Questa funzionalità non è presente in. AL2023

`ld.gold`Linker

Il `ld.gold` linker è disponibile in AL2 e viene rimosso in. AL2023 I clienti che creano software che fa riferimento esplicitamente al gold linker devono migrare al linker regular (). `ld.bfd`

Le note di rilascio originali di GNU Binutils per la versione 2.44 (rilasciata a febbraio 2025) documentano la rimozione di`ld.gold`: «Modificando la nostra prassi precedente, in questa versione l'archivio tar binutils-2.44.tar non contiene i sorgenti per il gold linker. Questo perché il gold linker è ora obsoleto e alla fine verrà rimosso a meno che i volontari non si facciano avanti e si offrano di continuare lo sviluppo e la manutenzione».

ping6

In AL2023, l'`ping`utilità normale supporta IPv6 nativamente e quella separata non `/bin/ping6` è più necessaria. In AL2023, `/usr/sbin/ping6` è un collegamento simbolico all'eseguibile. `/usr/bin/ping`

Questa modifica segue l'adozione da parte della comunità più ampia di `iputils` versioni più recenti che forniscono questa funzionalità, ad esempio la IPv6 modifica del Ping in Fedora.

`ftp`Package

Il `ftp` pacchetto in non AL2 è più disponibile in Amazon Linux a partire da AL2 023. Questa decisione è stata presa come parte del nostro costante impegno per la sicurezza, la manutenibilità e le moderne pratiche di sviluppo del software. Come parte (o prima) della migrazione a AL2 023, consigliamo di migrare qualsiasi utilizzo del `ftp` pacchetto legacy a una delle sue alternative.

Contesto

Il `ftp` pacchetto legacy non viene mantenuto attivamente a monte da molti anni. L'ultimo aggiornamento significativo del codice sorgente è avvenuto all'inizio degli anni 2000 e l'archivio dei sorgenti originale non è più disponibile. Sebbene alcune distribuzioni Linux abbiano installato patch per le vulnerabilità di sicurezza, la codebase rimane in gran parte non gestita.

Alternative consigliate

AL2023 offre diverse alternative moderne e gestite attivamente per la funzionalità FTP:

`lftp`(disponibile nelle versioni 023 AL2 e 023 AL2)

Un sofisticato programma di trasferimento file che supporta FTP, HTTP, SFTP e altri protocolli. Offre più funzionalità rispetto al `ftp` client tradizionale e viene mantenuto attivamente.

Installa con: dnf install lftp

`curl`(disponibile nelle versioni AL2 023 AL2 e 03)

Uno strumento a riga di comando versatile per il trasferimento di dati con URLs, che supporta FTP, FTPS, HTTP, HTTPS e molti altri protocolli.

Disponibile per impostazione predefinita in 023 tramite il pacchetto AL2. `curl-minimal` Per un supporto più esteso dei protocolli, puoi opzionalmente passare a `curl-full` using. dnf swap curl-minimal curl-full

`wget`(disponibile nelle versioni AL2 0 AL2 e 023)

Un'utilità da riga di comando non interattiva per scaricare file dal Web, che supporta i protocolli HTTP, HTTPS e FTP.

Installa con: dnf install wget (non installato di default in tutte le 023 immagini) AL2

`sftp`(disponibile nelle versioni AL2 0 AL2 e 023)

Un protocollo di trasferimento file sicuro che opera tramite SSH e fornisce trasferimenti di file crittografati.

Disponibile per impostazione predefinita come parte del pacchetto OpenSSH.

Considerazioni sulla migrazione

Se le applicazioni o gli script dipendono dal `ftp` client legacy, prendi in considerazione i seguenti approcci di migrazione:

1. Aggiorna gli script per utilizzare alternative moderne: modifica gli script per utilizzare`lftp`, `curl``wget`, o `sftp` al posto del client legacy. `ftp`
2. Esamina le dipendenze dei pacchetti: alcune applicazioni possono elencare il `ftp` pacchetto come dipendenza nei metadati del pacchetto, anche se da tempo sono migrate internamente all'utilizzo di protocolli moderni. In questi casi, l'applicazione potrebbe funzionare correttamente su AL2 023 nonostante la mancanza di elementi nel pacchetto. `/usr/bin/ftp` `ftp` Esamina i requisiti effettivi dell'applicazione anziché fare affidamento esclusivamente sulle dipendenze dichiarate.

3. Aggiorna le dipendenze delle applicazioni: per le applicazioni che gestisci che dichiarano ancora una dipendenza dal `ftp` pacchetto ma non lo utilizzano effettivamente, aggiorna i metadati del pacchetto per rimuovere questa dipendenza non necessaria.

Considerazioni sulla sicurezza

Il protocollo FTP trasmette i dati, incluse le credenziali di autenticazione, in testo semplice. Per le applicazioni sensibili alla sicurezza, consigliamo vivamente di utilizzare alternative crittografate come SFTP o HTTPS, supportate dagli strumenti alternativi consigliati.

Prepara la migrazione alla versione AL2 023

Puoi preparare il passaggio alla versione AL2 023 mentre continui a utilizzarla. AL2

Argomenti

Controlla l'elenco delle modifiche apportate alla versione 023 AL2

La documentazione AL2 023 contiene un elenco dettagliato delle modifiche che sono state implementate da allora. AL2 Queste informazioni sono disponibili nella sezione Confronto AL2 e AL2 023. È inoltre disponibile un elenco completo delle modifiche ai pacchetti software nella sezione Package changes in AL2 023.

AL2023 non include. `amazon-linux-extras` Fornisce invece pacchetti con namespace in cui vengono fornite più versioni. Poiché molti pacchetti vengono aggiornati nella versione AL2 023, le versioni di base in AL2 023 potrebbero essere successive alle versioni da cui state ricevendo. `amazon-linux-extras`

> **Note**
>
> Ti consigliamo di non eseguirla`amazon-linux-extras`, perché è EOL.

Dopo aver esaminato queste sezioni della documentazione, è possibile determinare se vi sono modifiche in AL2 023 che potrebbero richiedere l'adattamento dell'ambiente per la migrazione. Ad esempio, potrebbe essere necessario migrare finalmente uno script Python 2.7 in Python 3.

Esegui la migrazione ai timer da Jobs **`systemd cron`**

Per impostazione predefinita, non `cron` è installato nella AL2 versione 023. Puoi migrare i tuoi `cron` lavori su `systemd` Timer in preparazione alla migrazione AL2 a 023. AL2 `systemd`presenta molti vantaggi, come un controllo più preciso sull'esecuzione dei timer e una migliore registrazione.

AL2 Limitazioni

I seguenti argomenti trattano varie limitazioni di AL2 Amazon Linux e se sono state risolte in una versione più recente di Amazon Linux.

Argomenti

yumnon può verificare le firme GPG create con sottochiavi GPG

La versione del gestore di `rpm` pacchetti in AL2 è precedente all'`rpm`aggiunta del supporto per la verifica delle firme dei pacchetti create con le sottochiavi GPG. Se state creando pacchetti con cui essere compatibili AL2, dovrete assicurarvi di utilizzare chiavi di firma GPG compatibili con le chiavi di firma che fanno parte di `rpm` AL2

Per garantire la retrocompatibilità per gli utenti esistenti, la versione di `rpm` in AL2 riceve solo backport di sicurezza.

La versione di `rpm` in AL2 023 include il supporto per la verifica delle firme dei pacchetti create con le sottochiavi GPG.

Confronta AL1 e AL2

Negli argomenti seguenti vengono descritte le differenze principali tra AL1 e AL2. Contengono inoltre informazioni sulla durata e sul supporto e sulle modifiche ai pacchetti.

Argomenti

AL1 supporto ed EOL

AL1 ora è EOL. AL1 ha terminato il supporto standard il 31 dicembre 2020 ed era in fase di supporto alla manutenzione fino al 31 dicembre 2023.

Ti consigliamo di eseguire l'aggiornamento alla versione più recente di Amazon Linux.

Support per processori AWS Graviton

AL2 ha introdotto il supporto per i processori Graviton. AL2023 è ulteriormente ottimizzato per i processori Graviton.

`systemd` sostituisce **`upstart`** come sistema **`init`**

In AL2, `systemd` sostituito `upstart` come sistema. `init`

Python 2.6 e 2.7 sono stati sostituiti con Python 3

Sebbene Python 2.6 fosse AL1 contrassegnato come EOL nella versione 2018.03, i pacchetti erano ancora nei repository da installare. AL2 fornito con Python 2.7 come prima versione di Python supportata.

AL2023 completa la transizione a Python 3 e nessuna versione di Python 2.x è inclusa nei repository.

Confronto dei pacchetti installati su AL1 e AL2 AMIs

Pacchetto	AL1 AMI	AL2 AMI
GeoIP		1.5.0
PyYAML		3.10
acl	2,2,49	2,2,51
acpid	2.0,19	2.0,19
alsa-lib	1,0,22	
amazon-linux-extras		2.0.3
amazon-linux-extras-yum-plugin		2.0.3
amazon-ssm-agent	3.2.1705.0	3,21705,0
at	3,1,10	3,1,13
attr	2,4,46	2,4,46
audit	2,6,5	28.1
audit-libs	2,6,5	28.1
authconfig	6.2.8	6.2.8
aws-amitools-ec2	1,5,13	
aws-cfn-bootstrap	1.4	2.0
aws-cli	1,118,107	
awscli		1,184,7

Pacchetto	AL1 AMI	AL2 AMI
basesystem	10,0	10,0
bash	4,2,46	4,2,46
bash-completion		2.1
bc	1,006,95	1,006,95
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	
chkconfig	1,349,3	1,7,4

Pacchetto	AL1 AMI	AL2 AMI
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	16.7	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	
db4	4,7,25	

Pacchetto	AL1 AMI	AL2 AMI
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	0,63	0.7.3
dhclient	4.1.1	42,5
dhcp-common	4.1.1	42,5
dhcp-libs		42,5
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		30,20
dracut	004	033

Pacchetto	AL1 AMI	AL2 AMI
dracut-config-ec2		2.0
dracut-config-generic		033
dracut-modules-growroot	0.20	
dump	0.4	
dyninst		9,31
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
file	5,37	5,11

Pacchetto	AL1 AMI	AL2 AMI
file-libs	5,37	5,11
filesystem	2,4,30	3.2
findutils	44,2	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	29.2
gawk	3.1.7	40,2
gdbm	1.8.0	1.13
gdisk	0,8,10	0,8,10
generic-logos	17,0	18.0.0
get_reference_source	1.2	
gettext		0,198,1
gettext-libs		0,198,1
giflib	41.6	
glib2	2,36,3	2,56,1
glibc	2,17	2,26
glibc-all-langpacks		2,26

Pacchetto	AL1 AMI	AL2 AMI
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
gssproxy		0.7.0

Pacchetto	AL1 AMI	AL2 AMI
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)
java-1.7.0-openjdk	1,7,0,321	

Pacchetto	AL1 AMI	AL2 AMI
javapackages-tools	0.9.1	
jbigkit-libs		2.0
jpackage-utils	1,7,5	
json-c		0,11
kbd	1.15	1,15,5
kbd-legacy		1,15,5
kbd-misc	1.15	1,15,5
kernel	4,14,326	5,10,199
kernel-tools	4,14,326	5,10,199
keyutils	1,5,8	1.5.8
keyutils-libs	1.5.8	1.5.8
kmod	14	25
kmod-libs	14	25
kpartx	0,49	0,49
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
lcms2	2.6	

Pacchetto	AL1 AMI	AL2 AMI
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	0,3109	0,3109
libassuan	2.0.3	2.1.0
libattr	2,4,46	2,4,46
libbasicobjects		0,11
libblkid	2,23,2	2,30,2
libcap	2,16	2,54
libcap-ng	0,7,5	0,7,5

Pacchetto	AL1 AMI	AL2 AMI
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
libfontenc	1.0.5	

Pacchetto	AL1 AMI	AL2 AMI
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		0,13
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	
libnl	1.1.4	

Pacchetto	AL1 AMI	AL2 AMI
libnl3		3,2,28
libnl3-cli		3,2,28
libpath_utils		0,21
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
libsss_nss_idmap		1,16,5

Pacchetto	AL1 AMI	AL2 AMI
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		40,3
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	02,5
libverto-libevent		02,5
libwebp		0,3,0
libxcb	1.11	
libxml2	29.1	29.1

Pacchetto	AL1 AMI	AL2 AMI
libxml2-python		29.1
libxml2-python27	29.1	
libxslt	1,1,28	
libyaml	0,16	0,14
lm_sensors-libs		3.4.0
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3,7,8	38.6
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	26.3	26.3
man-pages	4,10	3,53
man-pages-overrides		7,5,2
mariadb-libs		5,5,68
mdadm	3.2.6	4.0
microcode_ctl	2.1	2.1

Pacchetto	AL1 AMI	AL2 AMI
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
nss-sysinit	3,53,1	3,90,0

Pacchetto	AL1 AMI	AL2 AMI
nss-tools	3,53,1	3,90,0
nss-util	3,53,1	3,90,0
ntp	4.2.8 p15	
ntpdate	4.2.8 p15	
ntsysv	1,349,3	1,7,4
numactl	2.0.7	
numactl-libs		2.0.9
openldap	2,4,40	2,4,44
openssh	7,4p 1	7,4p1
openssh-clients	7,4p1	7,4p1
openssh-server	7,4p1	7,4p1
openssl	1,0,2k	1,0,2k
openssl-libs		1,0,2k
os-prober		1.58
p11-kit	0,185	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	
pam_passwdqc	1.0.5	

Pacchetto	AL1 AMI	AL2 AMI
parted	2.1	3.1
passwd	0,79	0,79
pciutils	3,1,10	35,1
pciutils-libs	3,1,10	35,1
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
perl- PathTools	3,40	3,40

Pacchetto	AL1 AMI	AL2 AMI
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
Testo in Perl- ParseWords	3.29	3,29
Tempo Perl- 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
plymouth		0,89

Pacchetto	AL1 AMI	AL2 AMI
plymouth-core-libs		0,89
plymouth-scripts		0,89
pm-utils	1.4.1	1.4.1
policycoreutils	2,1,12	2.5
popt	1.13	1.13
postfix		210.1
procmail	3,22	
procps	32,8	
procps-ng		3,3,10
psacct	63,2	6.6.1
psmisc	22,20	22,20
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0,5,3
pystache		0,5,3
python		2,7,18
python-babel		0.9.6
python-backports		1.0
python-backports-ssl_match_hostname		3.5.0.1
python-cffi		1.6.0

Pacchetto	AL1 AMI	AL2 AMI
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
python-pycparser		2.14

Pacchetto	AL1 AMI	AL2 AMI
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		0,39
python2-cryptography		17.2
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		0,19
python2-rpm		4.11.3
python2-rsa		3.4.1
python2-s3transfer		0,3,3
python2-setuptools		41,2,0
python2-six		1.11.0

Pacchetto	AL1 AMI	AL2 AMI
python27	2,7,18	
python27-PyYAML	3,10	
python27-babel	0.9.4	
python27-backports	1.0	
python27-backports-ssl_match_hostname	3,40,2	
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	0,31	
python27-jinja2	27.2	

Pacchetto	AL1 AMI	AL2 AMI
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	0,17	
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	36,27	
python27-simplejson	3.6.5	

Pacchetto	AL1 AMI	AL2 AMI
python27-six	1.8.0	
python27-urlgrabber	3,10	
python27-urllib3	1,24,3	
python27-virtualenv	15,10	
python3		3,7,16
python3-daemon		2.2.3
python3-docutils		0,14
python3-libs		3,7,16
python3-lockfile		0.11.0
python3-pip		202,2
python3-pystache		0,5,4
python3-setuptools		49,13
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
rmt	0.4	

Pacchetto	AL1 AMI	AL2 AMI
rng-tools	5	6.8
rootfiles	8.1	8.1
rpcbind	0,2,0	02,0
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	42,2	
rubygems20	2,014,1	
scl-utils		20130529

Pacchetto	AL1 AMI	AL2 AMI
screen	40,3	4.1.0
sed	4.2.1	4.2.2
selinux-policy		3,13,1
selinux-policy-targeted		3,13,1
sendmail	8,14,4	
setserial	2,17	2,17
setup	2,8,14	2,8,71
setuptool		1,19,11
sgpio	1,2,0,10	1,2,0,10
shadow-utils	4,14.2	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		101,5
system-release	2018,03	2

Pacchetto	AL1 AMI	AL2 AMI
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	3,09	
tzdata	2023 c	2023c
tzdata-java	2023c	
udev	173	
unzip	6.0	6.0

Pacchetto	AL1 AMI	AL2 AMI
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	90,2081
vim-data	9,0,1712	90,2081
vim-enhanced	9,0,1712	90,2081
vim-filesystem	9,0,1712	90,2081
vim-minimal	9,0,1712	90,2081
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	90,2081
xz	5.2.2	5.2.2

Pacchetto	AL1 AMI	AL2 AMI
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

Confronto tra pacchetti installati AL1 e immagini dei container di AL2 base

Pacchetto	AL1 Contenitore	AL2 Contenitore
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
chkconfig	1,349,3	1,7,4

Pacchetto	AL1 Contenitore	AL2 Contenitore
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	40,2
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
gmp	6.0.0	6.0.0

Pacchetto	AL1 Contenitore	AL2 Contenitore
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
libgcc72	7.2.1	

Pacchetto	AL1 Contenitore	AL2 Contenitore
libgcrypt	1.5.3	1.5.3
libgpg-error	1.11	1.12
libicu	50,2	
libidn2	2.3.0	2.3.0
libmetalink		0,13
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	02,5
libxml2	29.1	29.1
libxml2-python27	29.1	
lua	5.1.4	5.1.4

Pacchetto	AL1 Contenitore	AL2 Contenitore
make	3,82	
ncurses	5.7	6.0
ncurses-base	5.7	6.0
ncurses-libs	5.7	6.0
nspr	4,25,0	4,35,0
nss	3,53,1	3,90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3,53,1	3,90,0
nss-softokn-freebl	3,53,1	3,90,0
nss-sysinit	3,53,1	3,90,0
nss-tools	3,53,1	3,90,0
nss-util	3,53,1	3,90,0
openldap	2,4,40	2,4,44
openssl	1,0,2k	
openssl-libs		1,0,2k
p11-kit	0,185	0,23,22
p11-kit-trust	0,18,5	0,23,22
pcre	8,21	8,32
pinentry	0,7,6	0.8.1
pkgconfig	0,27,1	

Pacchetto	AL1 Contenitore	AL2 Contenitore
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	0,31	
python27-kitchen	1.1.1	
python27-libs	2,7,18	
python27-pycurl	7,19,0	
python27-pygpgme	0.3	
python27-pyliblzma	0,5,3	
python27-pyxattr	0,5,0	
python27-urlgrabber	3,10	

Pacchetto	AL1 Contenitore	AL2 Contenitore
pyxattr		0,5,1
readline	6.2	6.2
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-python27	4.11.3	
sed	4.2.1	4.2.2
setup	2,8,14	2,8,71
shared-mime-info	1.1	1.8
sqlite	3,7,17	3,7,17
sysctl-defaults	1.0	
system-release	2018,03	2
tar	1,26	
tzdata	2023 c	2023c
vim-data		90,2081
vim-minimal		90,2081
xz-libs	5.2.2	5.2.2
yum	3.4.3	3.4.3
yum-metadata-parser	1.1.4	1.1.4
yum-plugin-ovl	1,1,31	1,1,31

Pacchetto	AL1 Contenitore	AL2 Contenitore
yum-plugin-priorities	1,1,31	1,1,31
yum-utils	1,1,31	
zlib	1.2.8	1.2.7

AL2 su Amazon EC2

> **Note**
>
> AL2 non è più la versione corrente di Amazon Linux. AL2023 è il successore di. AL2 Per ulteriori informazioni, vedere Confronto AL2 AL2023 e l'elenco delle modifiche al Package AL2023 nella Guida per l'AL2023 utente.

Argomenti

Avvia un'istanza Amazon EC2 con AMI AL2

Puoi avviare un'istanza Amazon EC2 con l'AMI AL2 . Per ulteriori informazioni, consulta Fase 1: Avvio di un'istanza.

Trova l' AL2 AMI più recente utilizzando Systems Manager

Amazon EC2 fornisce parametri AWS Systems Manager pubblici per il pubblico AMIs gestito da AWS che puoi utilizzare all'avvio delle istanze. Ad esempio, il parametro fornito da EC2 `/aws/service/`

`ami-amazon-linux-latest/amzn2-ami-kernel-default-hvm-x86_64-gp2` è disponibile in tutte le regioni e punta sempre alla versione più recente dell' AL2 AMI in una determinata regione.

Per trovare l' AL2023 AMI più recente utilizzata AWS Systems Manager, consulta la Guida introduttiva AL2023.

I parametri pubblici dell'AMI Amazon EC2 sono disponibili nel percorso seguente:

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

Puoi visualizzare un elenco di tutti gli Amazon Linux AMIs nella AWS regione corrente eseguendo il AWS CLI comando seguente.

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

Per avviare un'istanza mediante un parametro pubblico

L'esempio seguente utilizza il parametro pubblico fornito da EC2 per avviare un'`m5.xlarge`istanza utilizzando l'AMI AL2 più recente.

Per specificare il parametro nel comando, utilizzare la sintassi seguente: `resolve:ssm:`*`public-parameter`*, dove `resolve:ssm` è il prefisso standard e `public-parameter` è il percorso e il nome del parametro pubblico.

In questo esempio, i parametri `--count` e `--security-group` non sono inclusi. Per `--count`, il valore predefinito è 1. Se disponibili, un VPC predefinito e un gruppo di sicurezza predefinito vengono utilizzati.

```
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
```

Per ulteriori informazioni, consulta Using public parameters nella Guida per l'AWS Systems Manager utente.

Comprendere i nomi AMI di Amazon Linux 2

I nomi AMI di Amazon Linux 2 utilizzano il seguente schema di denominazione:

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

- Minimal AMIs viene fornito con un set ridotto al minimo di pacchetti preinstallati per ridurre le dimensioni dell'immagine.
- Kernel-version determina la versione del kernel preinstallata sulla rispettiva AMI:
  - `kernel-5.10`seleziona la versione 5.10 del kernel Linux. Questa è la versione del kernel consigliata per. AL2
  - `kernel-default`seleziona il kernel predefinito consigliato per. AL2 È un alias per kernel-5.10.
  - `kernel-4.14`seleziona la versione 4.14 del kernel Linux. Viene fornito solo per la compatibilità con le versioni AMI precedenti. Non utilizzare questa versione per il lancio di nuove istanze. Aspettatevi che questo AMI non sia più supportato.
  - Esiste un set speciale di nomi AMI senza riferimento a un kernel specifico. Si AMIs tratta di un alias per kernel-4.14. Questi AMIs sono forniti solo per la compatibilità con le versioni AMI precedenti. Non utilizzare questo nome AMI per il lancio di nuove istanze. Aspettatevi che il kernel li AMIs aggiorni.
- x86_64/aarch64 determina la piattaforma CPU su cui eseguire l'AMI. Seleziona x86_64 per le istanze EC2 basate su Intel e AMD. Seleziona aarch64 per le istanze Graviton EC2.
- ebs/gp2 determina il tipo di volume EBS utilizzato per servire il rispettivo AMI. Vedi Tipi di volume EBS per riferimento. Seleziona sempre gp2.

Connect a un'istanza Amazon EC2

Esistono diversi modi per connettersi alla tua istanza Amazon Linux, tra cui SSH ed EC2 Instance Connect. AWS Systems Manager Session Manager Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.

Utenti SSH e sudo

Amazon Linux non consente la shell `root` sicura remota (SSH) per impostazione predefinita. Inoltre, l'autenticazione tramite password è disabilitata per prevenire attacchi di forza bruta. Per abilitare i login SSH a un'istanza Amazon Linux, devi fornire la coppia di chiavi all'istanza all'avvio. Per consentire l'accesso SSH, devi anche impostare il gruppo di sicurezza utilizzato per avviare l'istanza. Per impostazione predefinita, l'unico account che può accedere in remoto tramite SSH è. `ec2-user` Anche questo account dispone sudo di privilegi. Se abiliti l'`root`accesso remoto, tieni presente che è meno sicuro che affidarsi a coppie di chiavi e a un utente secondario.

AL2 modalità di avvio AMI

AL2 AMIs non hanno un set di parametri per la modalità di avvio. Le istanze avviate da AL2 AMIs seguono il valore della modalità di avvio predefinito del tipo di istanza. Per ulteriori informazioni, consulta le modalità di avvio nella Guida per l'utente di Amazon EC2.

Archivio dei pacchetti

Queste informazioni si applicano a. AL2 Per informazioni su AL2023, consulta Gestire pacchetti e aggiornamenti del sistema operativo AL2023 nella Guida per l'utente di Amazon Linux 2023.

AL2 e AL1 sono progettati per essere utilizzati con repository di pacchetti online ospitati in ogni regione Amazon EC2. AWS Gli archivi sono disponibili in tutte le regioni ed è possibile accedervi tramite gli strumenti di aggiornamento yum. L'hosting degli archivi in ogni regione consente di distribuire gli aggiornamenti rapidamente e senza costi di trasferimento dei dati.

> **Important**
>
> L'ultima versione di AL1 ha raggiunto l'EOL il 31 dicembre 2023 e non riceverà aggiornamenti di sicurezza o correzioni di bug a partire dal 1° gennaio 2024. Per ulteriori informazioni, consulta AMI Amazon Linux end-of-life.

Se non hai bisogno di conservare dati o personalizzazioni per le tue istanze, puoi avviare nuove istanze utilizzando l'AMI corrente. AL2 Se hai bisogno di conservare dati o personalizzazioni per le tue istanze, puoi gestire tali istanze tramite gli archivi di pacchetti Amazon Linux. Questi archivi contengono tutti i pacchetti aggiornati. Puoi scegliere di applicare questi aggiornamenti alle istanze in esecuzione. Le versioni precedenti dell'AMI e dei pacchetti di aggiornamento continuano a essere disponibili per l'uso, anche se vengono rilasciate nuove versioni.

> **Note**
>
> Per aggiornare e installare pacchetti senza accesso a Internet su un'istanza Amazon EC2, vedi Come posso aggiornare yum o installare pacchetti senza accesso a Internet sulle mie istanze Amazon EC2 in esecuzione, oppure? AL1 AL2 AL2023

Per installare i pacchetti, utilizza il comando seguente:

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

Se riscontri che Amazon Linux non include un'applicazione necessaria, installa l'applicazione direttamente nell'istanza Amazon Linux. Amazon Linux utilizza RPMs e yum per la gestione dei pacchetti e questo è probabilmente il modo più diretto per installare nuove applicazioni. Ti consigliamo come prima cosa di controllare se un'applicazione è disponibile nel nostro archivio Amazon Linux centrale perché numerose applicazioni vengono rese disponibili in tale posizione. Da lì, puoi aggiungere queste applicazioni alla tua istanza Amazon Linux.

Per caricare le applicazioni in un'istanza Amazon Linux in esecuzione, utilizzare scp o sftp e quindi configurare l'applicazione accedendo all'istanza. Le applicazioni possono essere caricate anche durante l'avvio dell'istanza tramite l'operazione PACKAGE_SETUP dal pacchetto cloud-init predefinito. Per ulteriori informazioni, consulta Utilizzo di cloud-init su AL2.

Aggiornamenti di sicurezza

Gli aggiornamenti di sicurezza vengono forniti utilizzando gli archivi dei pacchetti. Sia gli aggiornamenti di sicurezza che gli avvisi di sicurezza AMI aggiornati sono pubblicati in Amazon Linux Security Center. Per ulteriori informazioni sulle policy di sicurezza AWS o per segnalare un problema di sicurezza, consulta Sicurezza di AWS Cloud.

AL1 e AL2 sono configurati per scaricare e installare aggiornamenti di sicurezza critici o importanti al momento del lancio. Gli aggiornamenti del kernel non sono inclusi in questa configurazione.

Nel AL2023, questa configurazione è cambiata rispetto a AL1 e AL2. Per ulteriori informazioni sugli aggiornamenti di sicurezza per AL2023, consulta Aggiornamenti e funzionalità di sicurezza nella Guida per l'utente di Amazon Linux 2023.

Consigliamo di eseguire gli aggiornamenti necessari in base alle proprie esigenze dopo l'avvio. Ad esempio, potresti voler applicare tutti gli aggiornamenti (non solo gli aggiornamenti di sicurezza) al momento del lancio oppure valutare ogni aggiornamento e applicare solo quelli applicabili al tuo sistema. Questa impostazione viene controllata tramite la seguente cloud-init impostazione: `repo_upgrade` Il seguente frammento di codice della configurazione cloud-init illustra come puoi modificare le impostazioni nel testo dei dati utente che passi all'inizializzazione dell'istanza:

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

I valori possibili di `repo_upgrade` sono indicati di seguito:

`critical`

Applica gli aggiornamenti di sicurezza critici in sospeso.

`important`

Applica gli aggiornamenti di sicurezza critici e importanti in sospeso.

`medium`

Applica gli aggiornamenti di sicurezza critici, importanti e di media gravità in sospeso.

`low`

Applica tutti gli aggiornamenti di sicurezza in sospeso, inclusi gli aggiornamenti di sicurezza di bassa gravità.

`security`

Applica gli aggiornamenti in evidenza o aggiornati contrassegnati da Amazon come aggiornamenti della sicurezza.

`bugfix`

Applica gli aggiornamenti contrassegnati da Amazon come correzioni di bug. Le correzioni di bug sono set più grandi di aggiornamenti, contenenti aggiornamenti della sicurezza e correzioni di numerosi altri bug secondari.

`all`

Applica tutti gli aggiornamenti disponibili applicabili, indipendentemente dalla relativa classificazione.

`none`

Non applica alcun aggiornamento all'istanza all'avvio.

> **Nota**
>
> Amazon Linux non contrassegna alcun aggiornamento come`bugfix`. Per applicare aggiornamenti non relativi alla sicurezza da Amazon Linux, usa`repo_upgrade: all`.

L'impostazione di default per `repo_upgrade` è security. Ciò significa che se non specifichi un valore diverso nei dati utente, per impostazione predefinita Amazon Linux esegue l'aggiornamento della sicurezza all'avvio per qualsiasi pacchetto attualmente installato. Amazon Linux ti notifica anche di eventuali aggiornamenti ai pacchetti installati elencando il numero di aggiornamenti disponibili al momento dell'accesso utilizzando il file `/etc/motd`. Per installare questi aggiornamenti, è necessario eseguire sudo yum upgrade sull'istanza.

Configurazione dell'archivio

For AL1 and AL2, AMIs sono un'istantanea dei pacchetti disponibili al momento della creazione dell'AMI, ad eccezione degli aggiornamenti di sicurezza. Tutti i pacchetti non presenti nell'AMI originale, ma installati in fase di esecuzione, saranno la versione più recente disponibile. Per ottenere i pacchetti più recenti disponibili per AL2, eseguiyum update -y.

> Suggerimento per la risoluzione dei problemi:
>
> Se si `cannot allocate memory` verifica un errore durante l'esecuzione yum update su tipi di istanze nano, ad esempio`t3.nano`, potrebbe essere necessario allocare lo spazio di swap per abilitare l'aggiornamento.

Infatti AL2023, la configurazione del repository è cambiata rispetto a e. AL1 AL2 Per ulteriori informazioni sul AL2023 repository, vedere Gestione dei pacchetti e degli aggiornamenti del sistema operativo.

Le versioni precedenti AL2023 erano configurate per fornire un flusso continuo di aggiornamenti da passare da una versione secondaria di Amazon Linux alla versione successiva, denominate anche release periodiche. Come best practice, ti consigliamo di aggiornare l'AMI all'ultima AMI disponibile anziché lanciare vecchi AMIs e applicare gli aggiornamenti.

Gli aggiornamenti sul posto non sono supportati tra le principali versioni di Amazon Linux, ad esempio from AL1 to AL2 o from AL2 to. AL2023 Per ulteriori informazioni, consulta Disponibilità Amazon Linux.

Utilizzo di cloud-init su AL2

Il pacchetto cloud-init è un'applicazione open source sviluppata da Canonical, che viene utilizzata per il bootstrap delle le immagini Linux in un ambiente di cloud computing, ad esempio Amazon EC2.

Amazon Linux include una versione personalizzata di cloud-init. Ciò consente di specificare le azioni da eseguire sull'istanza al momento dell'avvio. Puoi passare le operazioni desiderate al pacchetto cloud-init tramite i campi di dati utente all'avvio di un'istanza. Ciò significa che puoi utilizzare Common AMIs per molti casi d'uso e configurarli dinamicamente all'avvio. Amazon Linux utilizza inoltre cloud-init per eseguire la configurazione iniziale dell'account ec2-user.

Per ulteriori informazioni, consulta la documentazione cloud-init.

Amazon Linux utilizza le operazioni del pacchetto cloud-init disponibili in `/etc/cloud/cloud.cfg.d` e `/etc/cloud/cloud.cfg`. Puoi creare file di operazioni cloud-init personalizzati in `/etc/cloud/cloud.cfg.d`. Tutti i file presenti in questa directory vengono letti da cloud-init. Vengono letti in ordine alfabetico e i file più recenti sovrascrivono i valori dei file meno recenti.

Il pacchetto cloud-init esegue le seguenti attività di configurazione comuni e molte altre in fase di avvio:

- Impostare la lingua locale di default.
- Impostare il nome host.
- Analizzare e gestire i dati utente.
- Generare chiavi SSH private host.
- Aggiungere le chiavi SSH pubbliche di un utente a `.ssh/authorized_keys` per semplificare le procedure di login e amministrazione.
- Preparare gli archivi per la gestione dei pacchetti.
- Gestire le operazioni dei pacchetti definite nei dati utente.
- Esegui gli script utente presenti nei dati utente.
- Montare i volumi di instance store, se applicabile.
  - Per impostazione di default, il volume di instance store `ephemeral0` viene montato in `/media/ephemeral0`, se presente, e include un file system valido. In caso contrario, non viene montato.
  - Per impostazione di default, vengono montati i volumi di swap associati all'istanza (solo per i tipi di istanza `m1.small` e `c1.medium`).
  - Puoi sostituire il montaggio del volume di instance store di default con la seguente direttiva cloud-init:

```
#cloud-config
mounts:
```

```
- [ ephemeral0 ]
```

Per un maggiore controllo sui montaggi, consulta la sezione relativa al modulo Mounts nella documentazione di cloud-init.

- I volumi di instance store che supportano TRIM non vengono formattati quando viene avviata un'istanza. Pertanto, devi eseguire la partizione e la formattazione di tali volumi prima di poterli montare. Per ulteriori informazioni, consulta Instance Store Volume TRIM Support. Puoi utilizzare il modulo `disk_setup` per eseguire la partizione e la formattazione dei volumi di instance store all'avvio. Per ulteriori informazioni, consulta la sezione relativa al modulo Disk Setup nella documentazione di cloud-init.

Formati di dati utente supportati

Il pacchetto cloud-init supporta la gestione dei dati utente in una varietà di formati:

- Gzip
  - Se i dati utente sono compressi con gzip, cloud-init li decomprime e li gestisce in modo appropriato.
- MIME multipart
  - L'utilizzo di un file in formato MIME multipart ti consente di specificare più di un tipo di dati. Ad esempio, puoi specificare sia uno script di dati utente che un tipo di configurazione cloud. Ogni parte di un file in formato multipart può essere gestita da cloud-init se è uno dei formati supportati.
- Decodifica Base64
  - Se i dati utente sono codificati in base 64, cloud-init determina se è in grado di comprendere i dati decodificati come uno dei tipi supportati. Se è in grado di interpretare i dati decodificati, decodificherà i dati e li gestirà in modo appropriato. In caso contrario, restituirà i dati Base64 invariati.
- Script di dati utente
  - Inizia per `#!` o `Content-Type: text/x-shellscript`.
  - Lo script viene eseguito da `/etc/init.d/cloud-init-user-scripts` durante il primo ciclo di avvio. Ciò si verifica in una fase avanzata del processo di avvio, ovvero dopo l'esecuzione delle operazioni di configurazione iniziale.
- File di inclusione

  - Inizia per `#include` o `Content-Type: text/x-include-url`.
  - Questo contenuto è un file di inclusione. Il file contiene un elenco di, uno per riga. URLs Ciascuno di essi URLs viene letto e il relativo contenuto viene passato attraverso lo stesso insieme di regole. Il contenuto letto dall'URL può essere compresso con gzip o in testo MIME-multi-part semplice.
- Dati di configurazione del cloud
  - Inizia per `#cloud-config` o `Content-Type: text/cloud-config`.
  - Questo contenuto è costituito da dati di configurazione cloud.
- Upstart job (non supportato su) AL2
  - Inizia per `#upstart-job` o `Content-Type: text/upstart-job`.
  - Questo contenuto è archiviato in un file in `/etc/init` e upstart lo utilizza come fa con altri lavori upstart.
- Cloud Boothook
  - Inizia per `#cloud-boothook` o `Content-Type: text/cloud-boothook`.
  - Questo contenuto fa riferimento ai dati boothook. Viene memorizzato in un file in `/var/lib/cloud` e quindi eseguito immediatamente.
  - Si tratta dell'hook meno recente disponibile. Non è disponibile alcun meccanismo per eseguirlo solo una volta. Il boothook deve gestire questa situazione in autonomia. Viene fornito con l'ID istanza nella variabile di ambiente `INSTANCE_ID`. Usa questa variabile per fornire un once-per-instance set di dati boothook.

Configura le istanze AL2

Dopo aver avviato e effettuato correttamente l'accesso all' AL2 istanza, è possibile apportare modifiche all'istanza. Sono disponibili numerosi modi con cui puoi configurare un'istanza in base alle specifiche esigenze di un'applicazione. Di seguito sono riportate alcune attività comuni per iniziare a utilizzare le istanze.

Indice

- Cambia il nome host della tua istanza AL2
- Configura il DNS dinamico sulla tua istanza AL2
- Configura la tua interfaccia di rete usando ec2-net-utils per AL2

Scenari di configurazione comuni

La distribuzione di base di Amazon Linux contiene pacchetti software e utilità necessari per le operazioni di base del server. Tuttavia, numerosi altri pacchetti software sono disponibili in svariati archivi software, mentre nel codice sorgente sono disponibili molti altri pacchetti pronti per lo sviluppo. Per ulteriori informazioni sull'installazione e sullo sviluppo di software da questa posizioni, consulta Gestisci il software sulla tua istanza AL2.

Le istanze Amazon Linux sono preconfigurate con un `ec2-user`, ma puoi decidere di aggiungere altri utenti che non dispongono dei privilegi avanzati. Per ulteriori informazioni sull'aggiunta e la rimozione di utenti, consulta Manage users on your Linux instance nella Amazon EC2 User Guide.

Se disponi di una rete con un nome di dominio registrato, puoi modificare il nome host di un'istanza in modo da identificarla come appartenente a tale dominio. Puoi inoltre modificare il prompt di sistema in modo da visualizzare un nome più significativo senza modificare le impostazioni del nome host. Per ulteriori informazioni, consulta Cambia il nome host della tua istanza AL2. Puoi configurare un'istanza per l'uso di un provider di servizi DNS dinamico. Per ulteriori informazioni, consulta Configura il DNS dinamico sulla tua istanza AL2.

Quando avvii un'istanza in Amazon EC2, hai la possibilità di trasferire all'istanza i dati utente che possono essere utilizzati per eseguire attività di configurazione di routine e anche per l'esecuzione di script all'avvio dell'istanza. Puoi trasferire due tipi di dati utente a Amazon EC2, ovvero le direttive cloud-init e gli script di shell. Per ulteriori informazioni, consulta Esegui comandi sulla tua Linux istanza all'avvio nella Guida per l'utente di Amazon EC2.

Gestisci il software sulla tua istanza AL2

La distribuzione di base di Amazon Linux contiene pacchetti software e utilità necessari per le operazioni di base del server.

Queste informazioni si applicano a AL2. Per informazioni su AL2023, consulta Gestire pacchetti e aggiornamenti del sistema operativo AL2023 nella Guida per l'utente di Amazon Linux 2023.

È importante tenere aggiornati i software. Molti pacchetti in una distribuzione Linux vengono aggiornati di frequente per correggere bug, aggiungere caratteristiche e proteggere il sistema da

exploit a livello di sicurezza. Per ulteriori informazioni, consulta Aggiorna il software dell'istanza sulla tua istanza AL2.

Per impostazione predefinita, AL2 le istanze vengono avviate con i seguenti repository abilitati:

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

Sebbene in questi repository siano disponibili molti pacchetti aggiornati da AWS, è possibile che un pacchetto da installare sia contenuto in un altro repository. Per ulteriori informazioni, consulta Aggiungi repository su un'istanza AL2. Per semplificare la ricerca e l'installazione di pacchetti negli archivi abilitati, consulta Trova e installa pacchetti software su un' AL2 istanza.

Non tutti i software sono disponibili nei pacchetti software memorizzati negli archivi. Alcuni archivi devono essere compilati su un'istanza dal relativo codice sorgente. Per ulteriori informazioni, consulta Preparati a compilare il software su un'istanza AL2.

AL2 le istanze gestiscono il proprio software utilizzando il gestore di pacchetti yum. Il programma di gestione di pacchetti YUM consente di installare, rimuovere e aggiornare il software, nonché gestire tutte le dipendenze per ogni pacchetto.

Indice

Aggiorna il software dell'istanza sulla tua istanza AL2

È importante tenere aggiornati i software. I pacchetti in una distribuzione Linux vengono aggiornati di frequente per correggere bug, aggiungere funzionalità e proteggere il sistema da exploit a livello di sicurezza. Quando stabilisci una connessione a un'istanza Amazon Linux dopo averla avviata per la prima volta, è possibile che venga visualizzato un messaggio in cui ti viene richiesto di aggiornare i pacchetti software per motivi di sicurezza. Questa sezione mostra come aggiornare l'intero sistema o solo un pacchetto.

Queste informazioni si applicano a AL2. Per informazioni su AL2023, consulta Gestire pacchetti e aggiornamenti del sistema operativo AL2023 nella Guida per l'utente di Amazon Linux 2023.

Per informazioni sulle modifiche e gli aggiornamenti di AL2, consulta le note di AL2 rilascio.

Per informazioni sulle modifiche e gli aggiornamenti di AL2023, consulta le note di AL2023 rilascio.

> **Important**
>
> Se hai avviato un'istanza EC2 che utilizza un'AMI Amazon Linux 2 in una sottorete IPv6 - only, devi connetterti all'istanza ed eseguirla. `sudo amazon-linux-https disable` Ciò consente all' AL2 istanza di connettersi al yum repository in S3 IPv6 tramite il servizio di patch http.

Per aggiornare tutti i pacchetti su un'istanza AL2

1. (Opzionale) Avviare una sessione con il comando screen nella finestra della shell. A volte si possono verificare interruzioni di rete che possono comportare l'interruzione della connessione SSH all'istanza. Se si verifica questa situazione durante un aggiornamento software particolarmente lungo, l'istanza rimane in uno stato non definito, anche se ripristinabile. La sessione avviata con il comando screen ti permette di continuare l'esecuzione dell'aggiornamento anche se la connessione viene interrotta. Potrai infatti ristabilire la connessione alla sessione in un secondo momento senza problemi.

   a. Eseguire il comando screen per avviare la sessione.

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

   b. Se la connessione alla sessione viene interrotta, rieseguire l'accesso all'istanza e visualizzare l'elenco delle schermate disponibili.

   ```
   [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. Riconnettersi alla schermata utilizzando il comando screen -r e l'ID di processo del comando precedente.

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

   d. Dopo aver utilizzato il comando screen, utilizzare il comando exit per chiudere la sessione.

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

2. Esegui il comando yum update. Puoi decidere di aggiungere il flag `--security` per applicare solo gli aggiornamenti di sicurezza.

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

3. Verifica i pacchetti elencati, digita **y** e premi Invio per accettare gli aggiornamenti. L'aggiornamento di tutti i pacchetti in un sistema può richiedere alcuni minuti. L'output yum riporta lo stato dell'aggiornamento durante la sua esecuzione.
4. (Facoltativo) Riavviate l'istanza per assicurarvi di utilizzare i pacchetti e le librerie più recenti dell'aggiornamento; gli aggiornamenti del kernel non vengono caricati finché non si verifica un riavvio. Anche gli aggiornamenti applicati a qualsiasi libreria `glibc` devono essere seguiti da un riavvio. Per gli aggiornamenti dei pacchetti che controllano i servizi, può essere sufficiente riavviare i servizi per rendere disponibili gli aggiornamenti. Tuttavia, il riavvio del sistema garantisce il completamento di tutti i precedenti aggiornamenti di librerie e pacchetti.

Per aggiornare un singolo pacchetto su un'istanza AL2

Utilizzare questa procedura per aggiornare un singolo pacchetto e le relative dipendente, ma non l'intero sistema.

1. Esegui il comando yum update con il nome del pacchetto da aggiornare.

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

2. Verifica le informazioni sul pacchetto visualizzate, digita **y** e premi Invio per accettare uno o più aggiornamenti. A volte nell'elenco potrebbero venire elencati più pacchetti se sono presenti dipendenze di pacchetti che devono essere risolte. L'output yum riporta lo stato dell'aggiornamento durante la sua esecuzione.
3. (Facoltativo) Riavviate l'istanza per assicurarvi di utilizzare i pacchetti e le librerie più recenti dell'aggiornamento; gli aggiornamenti del kernel non vengono caricati finché non si verifica un riavvio. Anche gli aggiornamenti applicati a qualsiasi libreria `glibc` devono essere seguiti da un riavvio. Per gli aggiornamenti dei pacchetti che controllano i servizi, può essere sufficiente riavviare i servizi per rendere disponibili gli aggiornamenti. Tuttavia, il riavvio del sistema garantisce il completamento di tutti i precedenti aggiornamenti di librerie e pacchetti.

Aggiungi repository su un'istanza AL2

Queste informazioni si applicano a. AL2 Per informazioni in merito AL2023, consulta Aggiornamenti deterministici tramite repository con versioni nella Guida per AL2023 l'utente di Amazon Linux 2023.

Per impostazione predefinita, le AL2 istanze vengono avviate con i seguenti repository abilitati:

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

Questi repository cotengono molti pacchetti che vengono aggiornati da Amazon Web Services; potrebbe essere presente un pacchetto che vuoi installare ma contenuto in un altro repository.

Per installare un pacchetto da un archivio diverso con yum, è necessario aggiungere le informazioni relative all'archivio nel file `/etc/yum.conf` o nel relativo file *`repository`*`.repo` all'interno della directory `/etc/yum.repos.d`. Puoi eseguire questa operazione manualmente, ma per la maggior parte degli archivi yum è disponibile il file *`repository`*`.repo` corrispondente nel relativo URL.

Per determinare gli archivi yum già installati

Generare l'elenco degli archivi yum installati con il seguente comando:

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

Nell'output risultante sono elencati gli archivi installati assieme al relativo stato. Per gli archivi abilitati viene visualizzato il numero di pacchetti in essi contenuti.

Per aggiungere un archivio yum a /etc/yum.repos.d

1. Cerca la posizione del file `.repo`. Ciò può dipendere dall'archivio che desideri aggiungere. In questo esempio, il file `.repo` è disponibile in `https://www.`*`example`*`.com/`*`repository`*`.repo`.
2. Aggiungi il repository con il comando yum-config-manager.

```
[ec2-user ~]$ sudo yum-config-manager --add-repo https://
www.example.com/repository.repo
Loaded plugins: priorities, update-motd, upgrade-helper
adding repo from: https://www.example.com/repository.repo
```

```
grabbing file https://www.example.com/repository.repo to /etc/
yum.repos.d/repository.repo
repository.repo                                          | 4.0 kB     00:00
repo saved to /etc/yum.repos.d/repository.repo
```

Dopo aver installato un archivio, devi abilitarlo come descritto nella procedura seguente.

Per abilitare un archivio yum in /etc/yum.repos.d

Utilizzare il comando yum-config-manager con il contrassegno `--enable` *repository*. Il comando seguente abilita l'archivio EPEL (Extra Packages for Enterprise Linux) dal progetto Fedora. Per impostazione predefinita, questo archivio è presente in `/etc/yum.repos.d` nelle istanze di AMI Amazon Linux ma non è abilitato.

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

Per ulteriori informazioni e per scaricare la versione più recente di questo pacchetto, consultate https://fedoraproject. org/wiki/EPEL.

Trova e installa pacchetti software su un' AL2 istanza

Puoi utilizzare uno strumento di gestione dei pacchetti per trovare e installare pacchetti software. In Amazon Linux 2, lo strumento di gestione dei pacchetti software predefinito èYUM. In AL2023, lo strumento di gestione dei pacchetti software predefinito èDNF. Per ulteriori informazioni, consulta lo strumento di gestione dei pacchetti nella Guida per l'utente di Amazon Linux 2023.

Trova pacchetti software su un' AL2 istanza

Puoi utilizzare il comando yum search per cercare le descrizioni dei pacchetti disponibili negli archivi configurati. Ciò risulta particolarmente utile se non conosci il nome preciso del pacchetto che vuoi installare. Devi semplicemente aggiungere la ricerca per parola chiave alla fine del comando. Per ricerche di più parole, racchiudi la query di ricerca tra virgolette.

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

Di seguito è riportato un output di esempio.

```
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
```

Le query di ricerca di più parole racchiuse tra virgolette restituiscono solo i risultati che corrispondono esattamente alla query. Se il pacchetto previsto non viene visualizzato, semplifica la ricerca usando un'unica parola chiave e quindi riesamina i risultati. Come parole chiave puoi anche usare sinonimi per ampliare la ricerca.

Per ulteriori informazioni sui pacchetti per AL2, consulta quanto segue:

- AL2 Libreria Extras
- Archivio dei pacchetti

Installare pacchetti software su un' AL2 istanza

In AL2, lo strumento di gestione dei pacchetti yum cerca diversi pacchetti software in tutti gli archivi abilitati e gestisce eventuali dipendenze nel processo di installazione del software. Per informazioni sull'installazione di pacchetti software in AL2023, consulta Gestione dei pacchetti e degli aggiornamenti del sistema operativo nella Guida per l'utente di Amazon Linux 2023.

Per installare un pacchetto da un repository

Usa il yum install ***package*** comando, sostituendolo *package* con il nome del software da installare. Ad esempio, per installare il browser Web basato sul testo links, immetti il comando seguente.

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

Per installare i file dei pacchetti RPM scaricati

Puoi utilizzare yum install anche per installare i file dei pacchetti RPM scaricati da Internet. A tale scopo, devi aggiungere il nome del percorso di un file RPM al comando di installazione invece del nome del pacchetto di un repository.

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

Per elencare i pacchetti installati

Per visualizzare un elenco dei pacchetti installati nell'istanza, utilizzare il comando seguente.

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

Preparati a compilare il software su un'istanza AL2

In Internet è disponibile il software open source non precompilato e pronto per il download da un repository di pacchetti. Potresti tuttavia trovare un pacchetto software che devi compilare personalmente dal relativo codice sorgente. Affinché il tuo sistema sia in grado di compilare software in AL2 Amazon Linux, devi installare diversi strumenti di sviluppo, come makegcc, eautoconf.

Dal momento che la compilazione del software non è un'attività richiesta da ogni istanza di Amazon EC2, questi strumenti non vengono installati per impostazione predefinita, ma sono disponibili in un gruppo di pacchetti denominato "Development Tools" (Strumenti di sviluppo), che può essere facilmente aggiunto a un'istanza con il comando yum groupinstall.

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

I pacchetti di codice sorgente del software sono spesso disponibili per il download (da siti Web come https://github.com/e http://sourceforge.net/) come file di archivio compresso, chiamato tarball. In genere i file tarball sono associati all'estensione `.tar.gz`. Puoi decomprimere questi archivi tramite il comando tar.

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

Dopo aver decompresso ed estratto il pacchetto di codice sorgente, devi cercare un file `README` o `INSTALL` nella directory del codice sorgente contenente ulteriori istruzioni relative alla compilazione e all'installazione del codice sorgente.

Per recuperare il codice sorgente per i pacchetti Amazon Linux

Amazon Web Services fornisce il codice sorgente per i pacchetti mantenuti. Puoi scaricare il codice sorgente per qualsiasi pacchetto installato tramite il comando yumdownloader --source.

Eseguite il yumdownloader --source ***package*** comando per scaricare il codice sorgente di. *package* Ad esempio, per scaricare il codice sorgente del pacchetto `htop`, immetti il seguente comando.

```
[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
```

La posizione del file RPM sorgente è la directory da cui hai eseguito il comando.

Controllo dello stato del processore per la tua istanza Amazon EC2 AL2

Gli stati C-state controllano i livelli di sospensione in cui può entrare un core quando è inattivo. Gli stati C-state sono numerati a partire da C0 (lo stato più superficiale in cui il core è completamente attivo ed esegue le istruzioni) fino a C6 (lo stato inattivo più profondo in cui un core è spento).

Gli stati P-state controllano le prestazioni desiderate (in frequenza CPU) da un core. Gli stati P-state sono numerati a partire da P0 (l'impostazione sulle prestazioni più elevate in cui è permesso al core di utilizzare la tecnologia Intel Turbo Boost per aumentare la frequenza, se possibile) e vanno da P1 (lo stato P-state che richiede la frequenza di base massima) a P15 (la frequenza più bassa possibile).

Potresti modificare le impostazioni degli stati C-state o P-state per aumentare la consistenza delle prestazioni del processore, ridurre la latenza oppure ottimizzare l'istanza per un carico di lavoro specifico. Le impostazioni predefinite degli stati C-state e P-state forniscono le prestazioni massime, ottimali per la maggior parte dei carichi di lavoro. Tuttavia, se l'applicazione traesse vantaggio dalla

latenza ridotta al costo di frequenze single-core o dual-core più elevate o da prestazioni coerenti a frequenze più basse anziché frequenze Turbo Boost intermittenti, consigliamo di prendere in considerazione le impostazioni degli stati C-state o P-state disponibili per queste istanze.

Per informazioni sui tipi di istanze Amazon EC2 che consentono al sistema operativo di controllare gli stati C e P del processore, consulta Controllo dello stato del processore per l'istanza Amazon EC2 nella Guida per l'utente di Amazon EC2.

Le sezioni seguenti descrivono le diverse configurazioni di stato del processore e come monitorare gli effetti della configurazione. Queste procedure sono state scritte e si applicano ad Amazon Linux; tuttavia, potrebbero funzionare anche per altre distribuzioni Linux con una versione del kernel Linux 3.9 o successiva.

> **Note**
>
> Gli esempi presenti in questa pagina utilizzano quanto segue:
>
> - L'utilità turbostat per visualizzare la frequenza del processore e le informazioni sullo stato C. L'utilità turbostat è disponibile per impostazione predefinita su Amazon Linux.
> - Il comando stress per simulare un carico di lavoro. Per installare stress, per prima cosa abilitare il repository EPEL eseguendo sudo amazon-linux-extras install epel, poi eseguire sudo yum install -y stress.
>
> Se l'output non visualizza le informazioni sullo stato C, includere l'opzione --debug nel comando (sudo turbostat --debug stress ***<options>***).

Indice

Prestazioni massime con la massima frequenza Turbo Boost

Questa è la configurazione di controllo degli stati del processore predefinita per AMI Amazon Linux ed è consigliata per la maggior parte dei carichi di lavoro. Questa configurazione offre le prestazioni più elevate con minore variabilità. Permettendo ai core non attivi di entrare in stati di sospensione

più profondi fornisce la capacità aggiuntiva termica richiesta per processi single-core o dual-core per raggiungere il massimo potenziale Turbo Boost.

Il seguente esempio mostra un'istanza `c4.8xlarge` con due core attivamente in funzione che raggiungono la frequenza massima Turbo Boost del processore.

```
[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 questo esempio, v CPUs 21 e 28 funzionano alla frequenza Turbo Boost massima perché gli altri core sono entrati in stato di C6 sospensione per risparmiare energia e fornire spazio di alimentazione e calore ai core funzionanti. Le v CPUs 3 e 10 (ognuna delle quali condivide un core del processore con le v CPUs 21 e 28) sono nello C1 stato in attesa di istruzioni.

Nell'esempio seguente, tutti i 18 core stanno lavorando attivamente, quindi non c'è spazio per il Turbo Boost massimo, ma funzionano tutti alla velocità «Turbo Boost all-core» di 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
...
```

Prestazioni elevate e bassa latenza tramite limitazione degli stati C-state più profondi

Gli stati C-state controllano i livelli di sospensione in cui potrebbe entrare un core quando è inattivo. Potresti voler controllare gli stati C-state per ottimizzare la latenza rispetto alle prestazioni del sistema. Inserire i core nello stato di sospensione richiedete del tempo. Sebbene un core sospeso consenta maggiore capacità aggiuntiva per un altro core per raggiungere una frequenza più elevata, è necessario del tempo affinché il core sospeso torni attivo e in funzione. Ad esempio, se un core assegnato per gestire le interruzioni di un pacchetto di rete è sospeso, potrebbe verificarsi un ritardo nel lavoro su tale interruzione. Puoi configurare il sistema in modo da non utilizzare gli stati C-states più profondi, riducendo non solo la latenza di reazione del processore, ma anche la capacità aggiuntiva disponibile per altri core per Turbo Boost.

Uno scenario comune per la disabilitazione degli stati di sospensione più profondi è un'applicazione di database Redis, la quale archivia il database nella memoria di sistema per il tempo di risposta alle query più rapido possibile.

Per limitare gli stati di sonno più profondi, attiva AL2

1. Aprire il file `/etc/default/grub` con un editor a scelta.

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

2. Modificare la riga `GRUB_CMDLINE_LINUX_DEFAULT` e aggiungere le opzioni `intel_idle.max_cstate=1` e `processor.max_cstate=1` per impostare `C1` come lo stato C più profondo per i core inattivi.

```
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
```

   L'opzione `intel_idle.max_cstate=1` configura il limite dello stato C per le istanze basate su Intel e l'opzione `processor.max_cstate=1` configura il limite dello stato C per le istanze basate su AMD. È consigliabile aggiungere entrambe le opzioni alla configurazione. Ciò consente di impostare il comportamento desiderato sia su Intel che su AMD tramite una singola configurazione.

3. Salvare il file e uscire dall'editor.
4. Eseguire il comando riportato di seguito per ricreare la configurazione di avvio.

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

5. Riavviare l'istanza per abilitare la nuova opzione del kernel.

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

Limitazione degli stati di sospensione più profondi in Amazon Linux AMI

1. Aprire il file `/boot/grub/grub.conf` con un editor a scelta.

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

2. Modificare la riga `kernel` della prima voce e aggiungere le opzioni `intel_idle.max_cstate=1` e `processor.max_cstate=1` per impostare `C1` come lo stato C più profondo per i core inattivi.

```
# 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
```

L'opzione `intel_idle.max_cstate=1` configura il limite dello stato C per le istanze basate su Intel e l'opzione `processor.max_cstate=1` configura il limite dello stato C per le istanze basate su AMD. È consigliabile aggiungere entrambe le opzioni alla configurazione. Ciò consente di impostare il comportamento desiderato sia su Intel che su AMD tramite una singola configurazione.

3. Salvare il file e uscire dall'editor.
4. Riavviare l'istanza per abilitare la nuova opzione del kernel.

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

Il seguente esempio mostra un'istanza `c4.8xlarge` con due core attivamente in funzione alla frequenza del core "all core Turbo Boost".

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5322] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5322] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
  Pkg_W RAM_W PKG_% RAM_%
            5.56 3.20 2.90   0  94.44   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 131.90 31.11 199.47  0.00
 0   0   0   0.03 2.08 2.90   0  99.97   0.00   0.00   0.00   0.00   0.00   0.00   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 questo esempio, i core per le versioni CPUs 19 e 28 funzionano a 3.2 GHz e gli altri core sono `C1` nello stato C, in attesa di istruzioni. Sebbene i core in funzione non raggiungano la frequenza Turbo Boost massima, i core inattivi saranno molto più rapidi nella risposta a nuove richieste rispetto a quanto lo sarebbero nello stato C-state più profondo `C6`.

Prestazioni di base con la variabilità minore

Puoi ridurre la variabilità della frequenza del processore con gli stati P-state. Gli stati P-state controllano le prestazioni desiderate (in frequenza CPU) da un core. La maggior parte dei carichi di lavoro ottiene prestazioni migliori in P0, richiedendo Turbo Boost. Tuttavia, potresti voler ottimizzare il sistema per prestazioni coerenti anziché prestazioni intermittenti che possono verificarsi quando sono abilitate le frequenze Turbo Boost.

I carichi di lavoro Intel Advanced Vector Extensions (AVX o AVX2) possono funzionare bene a frequenze più basse e le istruzioni AVX possono consumare più energia. L'esecuzione del processore a una frequenza più bassa, disabilitando Turbo Boost, può ridurre la quantità di potenza e mantenere la velocità più coerente. Per ulteriori informazioni sull'ottimizzazione della configurazione dell'istanza e sul carico di lavoro per AVX, consulta il sito web Intel.

I driver inattivi della CPU controllano lo stato P. Le nuove generazioni di CPU richiedono driver inattivi della CPU aggiornati che corrispondono al livello del kernel come segue:

- Versioni del kernel Linux 6.1 e successive: supporta Intel Granite Rapids (ad esempio, R8i)
- Versioni del kernel Linux 5.10 e successive: supporta AMD Milan (ad esempio, M6a)
- Versioni del kernel Linux 5.6 e successive: supporta Intel Icelake (ad esempio, M6i)

Per verificare se il kernel del sistema in esecuzione riconosce la CPU, esegui il comando seguente.

```
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
```

Se l'output di questo comando indica una mancanza di supporto, consigliamo di aggiornare il kernel.

Questa sezione descrive come limitare gli stati di sospensione più profondi e come disabilitare Turbo Boost (richiedendo lo stato P-state `P1`) per fornire bassa latenza e la minima variabilità di velocità del processore per questi tipi di carichi di lavoro.

Per limitare gli stati di sonno più profondi e disattivare Turbo Boost su AL2

1. Aprire il file `/etc/default/grub` con un editor a scelta.

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

2. Modificare la riga `GRUB_CMDLINE_LINUX_DEFAULT` e aggiungere le opzioni `intel_idle.max_cstate=1` e `processor.max_cstate=1` per impostare `C1` come lo stato C più profondo per i core inattivi.

```
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
```

   L'opzione `intel_idle.max_cstate=1` configura il limite dello stato C per le istanze basate su Intel e l'opzione `processor.max_cstate=1` configura il limite dello stato C per le istanze basate su AMD. È consigliabile aggiungere entrambe le opzioni alla configurazione. Ciò consente di impostare il comportamento desiderato sia su Intel che su AMD tramite una singola configurazione.

3. Salvare il file e uscire dall'editor.
4. Eseguire il comando riportato di seguito per ricreare la configurazione di avvio.

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

5. Riavviare l'istanza per abilitare la nuova opzione del kernel.

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

6. Quando occorre la bassa variabilità di velocità del processore fornita dallo stato P-state `P1`, esegui il comando seguente per disabilitare Turbo Boost.

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

7. Una volta terminato il carico di lavoro, puoi riabilitare Turbo Boost con il comando seguente.

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

Limitazione degli stati di sospensione più profondi e disabilitazione di Turbo Boost in Amazon Linux AMI

1. Aprire il file `/boot/grub/grub.conf` con un editor a scelta.

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

2. Modificare la riga `kernel` della prima voce e aggiungere le opzioni `intel_idle.max_cstate=1` e `processor.max_cstate=1` per impostare `C1` come lo stato C più profondo per i core inattivi.

```
# 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
```

   L'opzione `intel_idle.max_cstate=1` configura il limite dello stato C per le istanze basate su Intel e l'opzione `processor.max_cstate=1` configura il limite dello stato C per le istanze basate su AMD. È consigliabile aggiungere entrambe le opzioni alla configurazione. Ciò consente di impostare il comportamento desiderato sia su Intel che su AMD tramite una singola configurazione.

3. Salvare il file e uscire dall'editor.
4. Riavviare l'istanza per abilitare la nuova opzione del kernel.

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

5. Quando occorre la bassa variabilità di velocità del processore fornita dallo stato P-state `P1`, esegui il comando seguente per disabilitare Turbo Boost.

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

6. Una volta terminato il carico di lavoro, puoi riabilitare Turbo Boost con il comando seguente.

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

L'esempio seguente mostra un'`c4.8xlarge`istanza con due v che lavora CPUs attivamente alla frequenza di base di base, senza 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
```

I core per le versioni CPUs 21 e 28 funzionano attivamente alla velocità di base del processore di 2,9 e anche tutti i core inattivi funzionano alla velocità di base nello stato C GHz, pronti ad accettare le istruzioni. `C1`

Scheduler I/O per AL2

Le I/O scheduler is a part of the Linux operating system that sorts and merges I/O richieste e determina l'ordine in cui vengono elaborate.

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/Ogli scheduler hanno un impatto minore sui dispositivi a stato solido e sugli ambienti virtualizzati. Questo perché per i

dispositivi solid state, l'accesso sequenziale e casuale non differisce e, per gli ambienti virtualizzati, l'host fornisce il proprio livello di pianificazione.

In questo argomento viene descritto lo I/O scheduler di Amazon Linux. Per ulteriori informazioni sul pianificatore I/O utilizzato da altre distribuzioni Linux, fare riferimento alla relativa documentazione.

Argomenti

Pianificatori supportati

Amazon Linux supporta i seguenti I/O programmi di pianificazione:

- `deadline`— Lo I/O scheduler Deadline ordina le I/O richieste e le gestisce nell'ordine più efficiente. Garantisce un orario di inizio per ogni I/O request. It also gives I/O richiesta rimasta in sospeso per troppo tempo e una priorità più alta.
- `cfq`— Lo I/O scheduler Completely Fair Queueing (CFQ) tenta di I/O resources between processes. It sorts and inserts I/O allocare equamente le richieste nelle code per processo.
- `noop`— Le I/O scheduler inserts all I/O richieste No Operation (noop) vengono inserite in una coda FIFO e poi le unisce in un'unica richiesta. Questo pianificatore non esegue l'ordinamento delle richieste.

Pianificatore di default

No Operation (noop) è lo I/O scheduler predefinito per Amazon Linux. Questo pianificatore viene utilizzato per i seguenti motivi:

- Molti tipi di istanza utilizzano dispositivi virtualizzati in cui l'host sottostante esegue la pianificazione dell'istanza.
- I dispositivi a stato solido vengono utilizzati in molti tipi di istanze in cui i vantaggi di uno I/O scheduler hanno un impatto minore.
- È lo I/O scheduler meno invasivo e può essere personalizzato se necessario.

Modifica del pianificatore

La modifica dello I/O scheduler può aumentare o diminuire le prestazioni a seconda che lo scheduler comporti il completamento di un numero maggiore o minore di I/O richieste in un determinato periodo di tempo. Ciò dipende in gran parte dal carico di lavoro, dalla generazione del tipo di istanza utilizzata e dal tipo di dispositivo a cui si accede. Se modifichi lo scheduler di I/O utilizzato, ti consigliamo di utilizzare uno strumento, come iotop, per misurare I/O le prestazioni e determinare se la modifica è vantaggiosa per il tuo caso d'uso.

È possibile visualizzare lo I/O scheduler di un dispositivo utilizzando il seguente comando, che utilizza come esempio. `nvme0n1` Sostituisci `nvme0n1` nel seguente comando con il dispositivo elencato in `/sys/block` nell'istanza.

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

Per impostare lo I/O scheduler per il dispositivo, utilizzare il seguente comando.

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

Ad esempio, per impostare lo I/O scheduler per un *xvda* dispositivo dal `noop` al`cfq`, utilizzate il comando seguente.

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

Cambia il nome host della tua istanza AL2

Quando avvii un'istanza in un VPC privato, Amazon EC2 assegna un nome host del sistema operativo guest. Il tipo di nome host assegnato da Amazon EC2 dipende dalle impostazioni della sottorete. Per ulteriori informazioni sui nomi host EC2, consulta i tipi di hostname delle istanze Amazon EC2 nella Amazon EC2 User Guide.

Un tipico nome DNS privato di Amazon EC2 per un'istanza EC2 configurata per utilizzare la denominazione basata su IP con un IPv4 indirizzo è simile al seguente:`ip-12-34-56-78.us-west-2.compute.internal`, dove il nome è composto dal dominio interno, dal servizio (in questo caso`compute`), dalla regione e da una forma dell'indirizzo privato. IPv4 Parte di questo nome host viene visualizzato nel prompt della shell quando esegui l'accesso all'istanza, ad esempio, `ip-12-34-56-78`). Ogni volta che si arresta e si riavvia l'istanza Amazon EC2 (a meno che non si utilizzi un indirizzo IP elastico), l' IPv4 indirizzo pubblico cambia, così come il nome DNS pubblico, il nome host del sistema e il prompt della shell.

> **Important**
>
> Queste informazioni si applicano ad Amazon Linux. Per informazioni su altre distribuzioni, consulta la documentazione specifica.

Modifica del nome host del sistema

Se disponi di un nome DNS pubblico registrato per l'indirizzo IP dell'istanza, ad esempio `webserver.mydomain.com`, puoi impostare il nome host del sistema in modo che l'istanza identifichi se stessa come appartenente a tale dominio. Ciò modifica anche il prompt della shell in modo che visualizzi la prima parte di questo nome anziché il nome host fornito da AWS (ad esempio,). `ip-12-34-56-78` Se non dispone di un nome DNS pubblico registrato, puoi comunque modificare il nome host, ma il processo necessario è leggermente diverso.

Affinché l'aggiornamento del nome host persista, è necessario verificare che l'impostazione cloud-init di `preserve_hostname` sia impostata su `true`. Per modificare o aggiungere questa impostazione è possibile eseguire il seguente comando:

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

Se l'impostazione `preserve_hostname` non è riportata, aggiungere la seguente riga di testo alla fine del file:

```
preserve_hostname: true
```

Per modificare il nome host del sistema in un nome DNS pubblico

Segui questa procedura se disponi già di un nome DNS pubblico registrato.

1.
   - Per AL2: utilizzate il hostnamectl comando per impostare il nome host in modo che rifletta il nome di dominio completo (ad esempio). **`webserver.mydomain.com`**

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

   - Per Amazon Linux AMI: nell'istanza, aprire il file di configurazione `/etc/sysconfig/network` nel proprio editor di testo preferito e modificare la voce `HOSTNAME` in base al nome di dominio completo, ad esempio **`webserver.mydomain.com`**.

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

2. Riavviare l'istanza per rendere effettivo il nuovo nome host.

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

   In alternativa puoi riavviare usando la console Amazon EC2 (nella pagina Instances (Istanze), seleziona l'istanza e scegli Instance state (Stato istanza), Reboot instance [Riavvia istanza]).

3. Eseguire l'accesso all'istanza e verificare che il nome host sia aggiornato. Il prompt deve mostrare il nuovo nome host (fino al primo ".") e il comando hostname deve mostrare il nome di dominio completo.

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

Per modificare il nome host del sistema senza un nome DNS pubblico

1.
   - Per AL2: utilizzare il hostnamectl comando per impostare il nome host in modo che rifletta il nome host di sistema desiderato (ad esempio). **`webserver`**

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

   - Per Amazon Linux AMI: nell'istanza, aprire il file di configurazione `/etc/sysconfig/network` nel proprio editor di testo preferito e modificare la voce `HOSTNAME` in base al nome host del sistema desiderato, ad esempio **`webserver`**.

```
HOSTNAME=webserver.localdomain
```

2. Aprire il file `/etc/hosts` nel proprio editor di testo preferito e modificare la voce che inizia con **`127.0.0.1`** in modo che corrisponda all'esempio seguente (sostituire con il proprio nome host).

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

3. Riavviare l'istanza per rendere effettivo il nuovo nome host.

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

In alternativa puoi riavviare usando la console Amazon EC2 (nella pagina Instances (Istanze), seleziona l'istanza e scegli Instance state (Stato istanza), Reboot instance [Riavvia istanza]).

4. Eseguire l'accesso all'istanza e verificare che il nome host sia aggiornato. Il prompt deve mostrare il nuovo nome host (fino al primo ".") e il comando hostname deve mostrare il nome di dominio completo.

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

Puoi anche implementare altre soluzioni programmatiche, ad esempio, specificare i dati utente per configurare l'istanza. Se l'istanza fa parte di un gruppo con scalabilità automatica, puoi utilizzare gli hook del ciclo di vita per definire i dati utente. Per maggiori informazioni, consulta Esecuzione di comandi sull'istanza Linux durante l'avvio e Hook del ciclo di vita per l'avvio delle istanze nella Guida per l'utente di AWS CloudFormation .

Modifica del prompt della shell senza ripercussioni sul nome host

Se non desiderate modificare il nome host della vostra istanza, ma desiderate che venga visualizzato un nome di sistema più utile (ad esempio**`webserver`**) rispetto al nome privato fornito da AWS (ad esempio,`ip-12-34-56-78`), potete modificare i file di configurazione del prompt della shell per visualizzare il nickname del sistema anziché il nome host.

Per modificare il prompt della shell in un nome host alternativo

1. Creare un file in `/etc/profile.d` in cui sia impostata la variabile di ambiente denominata `NICKNAME` sul valore che si desidera visualizzare nel prompt della shell. Ad esempio, per impostare il nome alternativo del sistema su **`webserver`**, esegui il comando seguente.

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

2. Aprire il file `/etc/bashrc` (Red Hat) o `/etc/bash.bashrc` (Debian/Ubuntu) con l'editor di testo preferito (ad esempio vim o nano). È necessario utilizzare sudo con il comando dell'editor in quanto `/etc/bashrc` e `/etc/bash.bashrc` sono di proprietà di `root`.
3. Modificare il file e la variabile del prompt della shell (`PS1`) in modo da visualizzare il nome alternativo anziché il nome host. Cercare la seguente riga che imposta il prompt della shell in `/`

`etc/bashrc` o `/etc/bash.bashrc`. Di seguito vengono visualizzate alcune righe circostanti per fornirne il contesto. Cercare la riga che inizia con `[ "$PS1"`):

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

Modificare \h (il simbolo per `hostname`) in tale riga impostando il valore della variabile `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. (Opzionale) Per impostare il titolo delle finestre della shell utilizzando il nuovo nome alternativo, completare la procedura seguente.

   a. Creare un file denominato `/etc/sysconfig/bash-prompt-xterm`.

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

   b. Rendere eseguibile il file utilizzando il seguente comando.

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

   c. Aprire il file `/etc/sysconfig/bash-prompt-xterm` con il proprio editor di testo preferito (ad esempio vim o nano). È necessario utilizzare sudo con il comando dell'editor in quando `/etc/sysconfig/bash-prompt-xterm` è di proprietà di `root`.

   d. Aggiungere la seguente riga al file.

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

5. Uscire e rieseguire l'accesso per rendere effettivo il nuovo valore del nome alternativo.

Modifica del nome host in altre distribuzioni Linux

Le procedure in questa pagina sono pensate per essere utilizzate solo con Amazon Linux. Per ulteriori informazioni su altre distribuzioni Linux, consulta la documentazione specifica e i seguenti articoli:

- How do I assign a static hostname to a private Amazon EC2 instance running RHEL 7 or Centos 7? (Come si assegna un nome host statico a un'istanza di Amazon EC2 privata eseguita in RHEL 7 o Centos 7?)

Configura il DNS dinamico sulla tua istanza AL2

Quando avvii un'istanza EC2, a tale istanza vengono assegnati un indirizzo IP pubblico e un nome del sistema dei nomi di dominio (DNS) pubblico che puoi utilizzare per raggiungere l'istanza da Internet. Dal momento che sono presenti numerosi host nel dominio di Amazon Web Services, questi nomi pubblici devono essere sufficientemente lunghi per garantirne l'univocità. Un tipico nome DNS pubblico di Amazon EC2 ha un aspetto simile al seguente:`ec2-12-34-56-78.us-west-2.compute.amazonaws.com`, dove il nome è composto dal dominio Amazon Web Services, dal servizio (in questo caso,`compute`) Regione AWS, e da una forma dell'indirizzo IP pubblico.

All'interno della relativa area del dominio, i servizi DNS dinamici forniscono nomi host DNS personalizzati facili da ricordare e che possono risultare più rilevanti per lo specifico caso d'uso dell'host. Inoltre, alcuni di questi servizi sono gratuiti. Puoi utilizzare un provider di servizi DNS dinamico con Amazon EC2 e configurare l'istanza per l'aggiornamento dell'indirizzo IP associato al nome DNS pubblico a ogni avvio dell'istanza. Sono disponibili numerosi provider selezionabili. I dettagli specifici relativi alla selezione di un provider e al suo utilizzo per la registrazione di un nome non rientrano nell'ambito della presente guida.

Per utilizzare il DNS dinamico con Amazon EC2

1. Eseguire la registrazione a un provider di servizi DNS dinamico e registrare un nome DNS pubblico mediante il relativo servizio. Questa procedura utilizza il servizio gratuito disponibile in noip.com/free come esempio.
2. Configurare il client di aggiornamento del DNS dinamico Dopo aver registrato un provider di servizi DNS dinamico e un nome DNS pubblico con il servizio, associare il nome DNS all'indirizzo IP dell'istanza. Numerosi provider, compreso noip.com, consentono di eseguire manualmente questa operazione dalla pagina dell'account nel proprio sito Web, ma molti altri supportano anche client di aggiornamento software. Se un client di aggiornamento è in

esecuzione su un'istanza EC2, il record del DNS dinamico viene aggiornato ogni volta che l'indirizzo IP cambia, come succede dopo un arresto e un riavvio. In questo esempio, viene installato il client noip2, che funziona con il servizio fornito da noip.com.

a. Abilita l'archivio Extra Packages for Enterprise Linux (EPEL) per accedere al client. `noip2`

> **Note**
>
> AL2 per impostazione predefinita, le istanze hanno le chiavi GPG e le informazioni del repository per l'archivio EPEL installate. Per ulteriori informazioni e per scaricare la versione più recente di questo pacchetto, consulta https://fedoraproject. org/wiki/EPEL.

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

b. Installare il pacchetto `noip`.

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

c. Creare il file di configurazione. Immettere le informazioni relativi al login e alla password quando viene richiesto e quindi rispondere alle domande successive per configurare il client.

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

3. Attivare il servizio noip.

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

4. Avviare il servizio noip.

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

Questo comando avvia il client, che legge il file di configurazione (`/etc/no-ip2.conf`) precedentemente creato e aggiorna l'indirizzo IP per il nome DNS pubblico selezionato.

5. Verificare che il client di aggiornamento abbia impostato l'indirizzo IP corretto per il nome DNS dinamico selezionato. Attendere alcuni minuti per consentire l'aggiornamento dei record DNS e

quindi provare a connettersi all'istanza utilizzando SSH con il nome DNS pubblico configurato in questa procedura.

Configura la tua interfaccia di rete usando ec2-net-utils per AL2

Amazon Linux 2 AMIs può contenere script aggiuntivi installati da AWS, noti come ec2-net-utils. Questi script automatizzano facoltativamente la configurazione delle interfacce di rete. Questi script sono disponibili solo per. AL2

> **Note**
>
> Per Amazon Linux 2023, il `amazon-ec2-net-utils` pacchetto genera configurazioni specifiche dell'interfaccia nella directory. `/run/systemd/network` Per ulteriori informazioni, consulta la sezione Servizio di rete nella Guida per l'utente di Amazon Linux 2023.

Usa il seguente comando per installare il pacchetto AL2 se non è già installato, oppure aggiornalo se è installato e sono disponibili aggiornamenti aggiuntivi:

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

I seguenti componenti fanno parte di ec2-net-utils:

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

Identifica le interfacce di rete quando vengono collegate, scollegate o ricollegate a un'istanza in esecuzione e assicura che lo script hotplug venga eseguito (`53-ec2-network-interfaces.rules`). Esegue la mappatura dell'indirizzo MAC a un nome di dispositivo (`75-persistent-net-generator.rules`, che genera `70-persistent-net.rules`).

Script hotplug

Genera un file di configurazione dell'interfaccia idoneo per l'utilizzo con DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Genera inoltre un file di configurazione del routing (`/etc/sysconfig/network-scripts/route-ethN`).

Script DHCP

Ogni volta che l'interfaccia di rete riceve un nuovo lease DHCP, questo script esegue una query sui metadati dell'istanza per cercare gli indirizzi IP elastici. Per ogni indirizzo IP elastico, aggiunge

una regola al database delle policy di routing per garantire che il traffico in uscita da tale indirizzo utilizzi l'interfaccia di rete corretta. All'interfaccia di rete aggiunge inoltre ciascun indirizzo IP privato come indirizzo secondario.

ec2ifup ethN (`/usr/sbin/`)

Estende la funzionalità del comando standard ifup. Dopo che questo script ha riscritto i file di configurazione `ifcfg-ethN` e `route-ethN`, esegue ifup.

ec2ifdown ethN (`/usr/sbin/`)

Estende la funzionalità del comando standard ifdown. Dopo che questo script ha rimosso le regole per l'interfaccia di rete dal database delle policy di routing, esegue ifdown.

ec2ifscan (`/usr/sbin/`)

Verifica la presenza di interfacce di rete non configurate e le configura.

Questo script non è disponibile nella versione iniziale di ec2-net-utils.

Per elencare i file di configurazione generati da ec2-net-utils, utilizzare il seguente comando:

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

Per disabilitare l'automazione, puoi aggiungere `EC2SYNC=no` al file `ifcfg-ethN` corrispondente. Ad esempio, utilizza il seguente comando per disabilitare l'automazione per l'interfaccia eth1:

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

Per disabilitare completamente l'automazione, puoi rimuovere il pacchetto utilizzando il seguente comando:

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

Kernel forniti dall'utente

Se ti occorre un kernel personalizzato per le istanze Amazon EC2, puoi iniziare con un'AMI vicina a quella che desideri, quindi puoi compilare il kernel personalizzato sull'istanza e aggiornare il bootloader per puntare al nuovo kernel. Questo processo varia a seconda del tipo di virtualizzazione

utilizzato dall'AMI. Per ulteriori informazioni, consulta i tipi di virtualizzazione delle AMI Linux nella Guida per l'utente di Amazon EC2.

Indice

HVM (AMIs GRUB)

I volumi delle istanze HVM vengono trattati come dischi fisici reali. Il processo di avvio è simile a quello di un sistema operativo bare metal, con un disco partizionato e un bootloader che consente di lavorare con tutte le distribuzioni Linux attualmente supportate. Il bootloader più comune è GRUB o. GRUB2

Per impostazione predefinita, GRUB non invia il suo output alla console dell'istanza, perché questo comporta un ritardo aggiuntivo nell'avvio. Per ulteriori informazioni, consulta Output della console delle istanze nella Guida per l'utente di Amazon EC2. Se si sta installando un kernel personalizzato, si dovrebbe prendere in considerazione l'abilitazione dell'output di GRUB.

Non occorre specificare un kernel di fallback, ma suggeriamo di averne uno quando si prova un nuovo kernel. GRUB può ritornare su un altro kernel nel caso in cui quello nuovo non funzioni. Avere un kernel di fallback consente l'avvio dell'istanza anche se il nuovo kernel non viene trovato.

La versione precedente di GRUB per Amazon Linux utilizza`/boot/grub/menu.lst`. GRUB2 per AL2 usi`/etc/default/grub`. Per ulteriori informazioni sull'aggiornamento del kernel predefinito nel bootloader, vedere la documentazione per la distribuzione Linux.

Paravirtual AMIs (PV-GRUB)

AMIs che utilizzano la virtualizzazione paravirtual (PV) utilizzano un sistema chiamato PV-GRUB durante il processo di avvio. PV-GRUB è un bootloader paravirtuale che esegue patch della versione GNU GRUB 0.97. Quando avvii un'istanza, PV-GRUB inizia il processo di avvio e carica in sequenza il kernel specificato dal file dell'immagine `menu.lst`.

PV-GRUB comprende i comandi standard `grub.conf` o `menu.lst`, che gli consentono di lavorare con tutte le distribuzioni Linux attualmente supportate. Le distribuzioni precedenti, come Ubuntu 10.04 LTS, Oracle Enterprise Linux o CentOS 5.x, richiedono uno speciale pacchetto di kernel "ec2" o "xen", mentre le distribuzioni più recenti includono i driver necessari nel pacchetto di kernel predefinito.

La maggior parte delle moderne AMI paravirtuali utilizza un AKI PV-GRUB per impostazione predefinita (comprese tutte le AMI Linux paravirtuali disponibili nel menu Amazon EC2 Launch Wizard Quick Start), perciò non occorre eseguire altri passaggi per utilizzare un kernel diverso sull'istanza, sempre che il kernel che vuoi utilizzare sia compatibile con la tua distribuzione. Il modo migliore per eseguire un kernel personalizzato sulla tua istanza è iniziare da un'AMI vicina a quella desiderata, quindi compilare il kernel personalizzato sull'istanza e modificare il file `menu.lst` per eseguire l'avvio con quel kernel.

È possibile verificare che l'immagine del kernel per un AMI sia un AKI PV-GRUB. Eseguire il comando describe-images (sostituendo l'ID immagine del kernel) e verificare se il campo `Name` inizia con `pv-grub`:

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

Indice

Limiti di PV-GRUB

PV-GRUB presenta i seguenti limiti:

- Non è possibile utilizzare la versione a 64 bit di PV-GRUB per avviare un kernel da 32 bit o viceversa.
- Non è possibile specificare una Amazon ramdisk image (ARI) quando si utilizza un AKI PV-GRUB.
- AWS ha testato e verificato che PV-GRUB funzioni con questi formati di file system: EXT2,,, JFS EXT3 EXT4, XFS e ReiserFS. Altri formati potrebbero non funzionare.
- PV-GRUB può avviare kernel compressi tramite i formati di compressione gzip, bzip2, lzo e xz.
- I cluster AMIs non supportano o non necessitano di PV-GRUB, poiché utilizzano la virtualizzazione hardware completa (HVM). Mentre le istanze paravirtuali utilizzano PV-GRUB per l'avvio, i volumi delle istanze HVM sono trattati come dischi reali e il processo di avvio è simile a quello di un sistema operativo bare metal con disco partizionato e bootloader.
- Le versioni 1.03 e precedenti di PV-GRUB non supportano il partizionamento GPT, ma solo il partizionamento MBR.

- Se hai in programma di utilizzare un gestore logico di volumi (LVM) con i volumi Amazon Elastic Block Store (Amazon EBS), ti servirà una partizione di avvio distinta al di fuori del LVM. Potrai così creare volumi logici con il LVM.

Configura GRUB per paravirtual AMIs

Per avviare PV-GRUB, nell'immagine deve essere presente un file `menu.lst` GRUB; la posizione più comune di questo file è `/boot/grub/menu.lst`.

Di seguito è riportato un esempio di un file di configurazione `menu.lst` per l'avvio di un'AMI con un AKI PV-GRUB. In questo esempio è possibile scegliere tra due voci di kernel: Amazon Linux 2018.03 (il kernel originale dell'AMI) e Vanilla Linux 4.16.4 (una versione più recente del kernel Vanilla Linux da https://www.kernel.org/). La voce Vanilla è stata copiata dalla voce originale di questa AMI e i percorsi `kernel` e `initrd` sono stati aggiornati sulle nuove posizioni. Il parametro `default 0` punta il bootloader sulla prima voce che visualizza (in questo caso, la voce Vanilla) e il parametro `fallback 1` punta il bootloader sulla voce successiva in caso di problemi nell'avvio della prima.

```
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
```

Non occorre specificare un kernel di fallback nel file `menu.lst`, ma ti suggeriamo di averne uno quando testi un nuovo kernel. PV-GRUB può ritornare su un altro kernel nel caso in cui quello nuovo non funzioni. Avere un kernel di fallback permette l'avvio dell'istanza anche se il nuovo kernel non viene trovato.

PV-GRUB controlla le seguenti posizioni di `menu.lst` utilizzando la prima che trova:

- `(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`

Le versioni di PV-GRUB fino alla 1.03 controllano solo una delle prime due posizioni nell'elenco.

Immagine del kernel Amazon PV-GRUB IDs

Gli AKI PV-GRUB sono disponibili in tutte le Regioni di Amazon EC2, esclusa la Regione Asia Pacifico (Osaka). Esistono tipi di architettura sia AKIs a 32 bit che a 64 bit. La maggior parte delle versioni moderne AMIs utilizza un PV-GRUB AKI di default.

Ti suggeriamo di utilizzare sempre la versione più recente dell'AKI PV-GRUB, perché non tutte le versioni sono compatibili con ogni tipo di istanza. Utilizzate il seguente comando describe-images per ottenere un elenco di PV-GRUB per la regione corrente: AKIs

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

PV-GRUB è l'unico AKI disponibile nella regione `ap-southeast-2`. Devi verificare che le AMI che vuoi copiare su questa regione utilizzino una versione di PV-GRUB disponibile nella regione.

Le seguenti sono le AKI correnti per ogni regione. IDs Registra un nuovo AMIs file usando un AKI hd0.

> **Note**
>
> Continuiamo a fornire hd00 AKIs per la retrocompatibilità nelle regioni in cui erano precedentemente disponibili.

ap-northeast-1, Asia Pacific (Tokyo)

ID immagine	Nome immagine
aki-f975a998	pv-grub-hd0_1.05-i386.gz
aki-7077ab11	pv-grub-hd0_1.05-x86_64.gz

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

ID immagine	Nome immagine
aki-17a40074	pv-grub-hd0_1.05-i386.gz
aki-73a50110	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-2, Asia Pacific (Sydney)

ID immagine	Nome immagine
aki-ba5665d9	pv-grub-hd0_1.05-i386.gz
aki-66506305	pv-grub-hd0_1.05-x86_64.gz

eu-central-1, Europe (Frankfurt)

ID immagine	Nome immagine
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1, Europe (Ireland)

ID immagine	Nome immagine
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz

ID immagine	Nome immagine
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1, South America (São Paulo)

ID immagine	Nome immagine
aki-7cd34110	pv-grub-hd0_1.05-i386.gz
aki-912fbcfd	pv-grub-hd0_1.05-x86_64.gz

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

ID immagine	Nome immagine
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 (Stati Uniti occidentali)

ID immagine	Nome immagine
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

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

ID immagine	Nome immagine
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2, US West (Oregon)

ID immagine	Nome immagine
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

Aggiornamento di PV-GRUB

Ti suggeriamo di utilizzare sempre la versione più recente dell'AKI PV-GRUB, perché non tutte le versioni sono compatibili con ogni tipo di istanza. Inoltre, le versioni precedenti di PV-GRUB non sono disponibili in tutte le regioni, quindi se copi un'AMI che utilizza una versione precedente su una regione che non la supporta, non potrai avviare istanze da quell'AMI fino a quando non aggiorni l'immagine del kernel. Utilizza le seguenti procedure per verificare la versione di PV-GRUB dell'istanza e aggiornarla se necessario.

Per verificare la versione di PV-GRUB

1. Trovare l'ID kernel per l'istanza.

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

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

   L'ID kernel per l'istanza è `aki-70cb0e10`.

2. Visualizzare le informazioni sulla versione dell'ID kernel.

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

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

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

L'immagine del kernel è PV-GRUB 1.05. Se la versione di PV-GRUB non è la più recente (come indicato in Immagine del kernel Amazon PV-GRUB IDs), devi aggiornarla utilizzando la seguente procedura.

Per aggiornare la versione di PV-GRUB

Se la tua istanza utilizza una versione precedente di PV-GRUB, devi aggiornarla alla versione più recente.

1. Identificare l'AKI PV-GRUB più recente per la regione e l'architettura del processore da Immagine del kernel Amazon PV-GRUB IDs.
2. Arrestare l'istanza. La tua istanza deve essere arrestata per modificare l'immagine del kernel utilizzata.

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

3. Modificare l'immagine del kernel utilizzata per l'istanza.

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

4. Riavviare l'istanza.

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

AL2 Notifiche di rilascio AMI

Per ricevere una notifica quando AMIs vengono rilasciati nuovi Amazon Linux, puoi abbonarti utilizzando Amazon SNS.

Per informazioni sulla sottoscrizione alle notifiche per AL2023, consulta Ricezione di notifiche sui nuovi aggiornamenti nella Guida per l'utente di Amazon Linux 2023.

> **Note**
>
> Il supporto standard per AL1 è terminato il 31 dicembre 2020. La fase AL1 di supporto alla manutenzione si è conclusa il 31 dicembre 2023. Per ulteriori informazioni sull' AL1 EOL e sul supporto di manutenzione, consulta il post del blog Update on Amazon Linux AMI end-of-life.

Per sottoscrivere alle notifiche Amazon Linux

1. Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. Devi selezionare la regione in cui la notifica SNS per la quale hai effettuato la sottoscrizione è stata creata.
3. Nel pannello di navigazione, scegli Subscriptions (Abbonamenti), quindi Create subscription (Crea abbonamento).
4. Nella finestra di dialogo Create subscription (Crea sottoscrizione) eseguire le seguenti operazioni:
   a. [AL2] In Topic ARN (ARN argomento) copiare e incollare il seguente ARN (Amazon Resource Name): **`arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates`**.
   b. [Amazon Linux] In Topic ARN (ARN argomento) copiare e incollare il seguente nome della risorsa Amazon (ARN): **`arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates`**.
   c. Per Protocol, scegliere Email.
   d. In Endpoint immetti l'indirizzo e-mail utilizzabile per ricevere le notifiche.
   e. Scegli Create Subscription (Crea sottoscrizione).
5. Riceverai un'e-mail di conferma con oggetto "AWS Notifica - Conferma dell'abbonamento». Apri l'e-mail e seleziona Conferma sottoscrizione per completare la sottoscrizione.

Ogni volta che AMIs vengono rilasciati, inviamo notifiche agli abbonati sull'argomento corrispondente. Per non ricevere più queste notifiche, utilizza la procedura seguente per annullare la sottoscrizione.

Per annullare la sottoscrizione alle notifiche Amazon Linux

1. Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/

2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario utilizzare la regione in cui è stata creata la notifica SNS.
3. Nel pannello di navigazione scegli Subscriptions (Abbonamenti), seleziona l'abbonamento, quindi scegli Actions (Operazioni), Delete subscriptions (Elimina sottoscrizioni).
4. Quando viene richiesta la conferma, seleziona Elimina.

Formato dei messaggi AMI SNS Amazon Linux

Lo schema per il messaggio SNS è il seguente.

```
{
    "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"
    ]
}
```

Configura la connessione desktop MATE AL2

L'ambiente desktop MATE è preinstallato e preconfigurato AMIs con la seguente descrizione:

".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)."

L'ambiente fornisce un'interfaccia utente grafica intuitiva per l'amministrazione delle istanze AL2 con un uso minimo della riga di comando. L'interfaccia utilizza rappresentazioni grafiche, come icone, finestre, barre degli strumenti, cartelle, sfondi e widget desktop. Sono disponibili strumenti integrati basati su GUI per eseguire attività comuni. Ad esempio, esistono strumenti per aggiungere e rimuovere software, applicare aggiornamenti, organizzare file, avviare programmi e monitorare lo stato del sistema.

> **Important**
>
> `xrdp` è il software per desktop remoto incluso nell'AMI. Per impostazione predefinita, `xrdp` utilizza un certificato TLS autofirmato per crittografare le sessioni di desktop remoto. AWS Né i `xrdp` manutentori consigliano di utilizzare certificati autofirmati in produzione. Al contrario, ottenere un certificato da un'autorità di certificazione (CA) appropriata e installarlo nelle istanze. Per ulteriori informazioni sulla configurazione TLS, consulta il livello di sicurezza TLS sulla wiki `xrdp`.

> **Note**
>
> Se preferisci utilizzare un servizio di elaborazione di rete virtuale (VNC) anziché xrdp, consulta l'articolo Come posso installare una GUI sulla mia istanza Amazon EC2 che esegue Knowledge Center. AL2 AWS

Prerequisito

Per eseguire i comandi mostrati in questo argomento, devi installare AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell e configurare il tuo profilo. AWS

Opzioni

1. Installa il AWS CLI : per ulteriori informazioni, consulta Installazione AWS CLI e nozioni di base sulla configurazione nella Guida per l'AWS Command Line Interface utente.
2. Installa gli strumenti per Windows PowerShell : per ulteriori informazioni, consulta Installazione AWS Tools for Windows PowerShell e condivisione delle credenziali nella Guida per l'AWS Strumenti per PowerShell utente.

> **Tip**
>
> In alternativa all'installazione completa di AWS CLI, è possibile utilizzare AWS CloudShelluna shell preautenticata basata su browser che si avvia direttamente da. Console di gestione AWS Seleziona Supportato Regioni AWS, per assicurarti che sia disponibile nella regione in cui lavori.

Configurazione della connessione RDP

Attieniti alla seguente procedura per impostare una connessione RDP (Remote Desktop Protocol) dal computer locale a un'istanza AL2 che esegue l'ambiente desktop MATE.

1. Per ottenere l'ID dell'AMI AL2 che include MATE nel nome AMI, puoi usare il comando describe-images dallo strumento a riga di comando locale. Se non avete installato gli strumenti da riga di comando, potete eseguire la seguente interrogazione direttamente da una sessione. AWS CloudShell Per informazioni su come avviare una sessione di shell da CloudShell, consultate Guida introduttiva AWS CloudShell. Dalla console Amazon EC2 è possibile trovare l'AMI che include MATE avviando un'istanza e quindi inserendo `MATE` nella barra di ricerca AMI. Il AL2 Quick Start con MATE preinstallato verrà visualizzato nei risultati della ricerca.

```
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"
    ]
]
```

   Scegli l'AMI appropriato per il tuo utilizzo.
2. Avviare un'istanza EC2 con l'AMI individuata nel passaggio precedente. Configurare il gruppo di sicurezza per consentire il traffico TCP in ingresso alla porta 3389. Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza per il VPC. Questa configurazione consente di utilizzare un client RDP per connettersi all'istanza.
3. Connettersi all'istanza utilizzando SSH.
4. Aggiorna il software e il kernel sull'istanza.

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

Al termine dell'aggiornamento riavvia l'istanza per accertarti che utilizzi i pacchetti e le librerie dell'aggiornamento; gli aggiornamenti del kernel vengono caricati solo dopo il riavvio.

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

5. Ricollegati all'istanza e utilizza il comando seguente sull'istanza Linux per impostare la password per `ec2-user`.

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

6. Installare il certificato e la chiave.

   Se già disponi di un certificato e di una chiave, copiali nella directory `/etc/xrdp/` come segue:

   - Certificato - `/etc/xrdp/cert.pem`
   - Chiave - `/etc/xrdp/key.pem`

   Se non disponi di un certificato e di una chiave, utilizza il seguente comando per generarli nella directory `/etc/xrdp`.

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

   > **Note**
   >
   > Questo comando genera un certificato valido per 365 giorni.

7. Aprire un client RDP sul computer da cui ci si connette all'istanza (ad esempio, Connessione desktop remoto su un computer che esegue Microsoft Windows). Immettere `ec2-user` come nome utente e immettere la password creata nella fase precedente.

Disabilitare **`xrdp`** sull'istanza Amazon EC2

È possibile disattivare `xrdp` in qualsiasi momento eseguendo uno dei seguenti comandi sull'istanza Linux. I seguenti comandi non influiscono sulla capacità di utilizzare MATE con un server X11.

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

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

Abilitare **`xrdp`** sull'istanza Amazon EC2

Per riattivarlo `xrdp` in modo da poterti connettere alla tua AL2 istanza che esegue l'ambiente desktop MATE, esegui uno dei seguenti comandi sull'istanza Linux.

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

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

AL2 Tutorial

I seguenti tutorial mostrano come eseguire attività comuni utilizzando istanze Amazon EC2 in esecuzione. AL2 Per i tutorial video, consulta Video didattici e laboratori.AWS

Per AL2023 istruzioni, consulta i tutorial nella Guida per l'utente di Amazon Linux 2023.

Esercitazioni

- Tutorial: installa un server LAMP su AL2
- Tutorial: Configura SSL/TLS su AL2
- Tutorial: Ospita un WordPress blog su AL2

Tutorial: installa un server LAMP su AL2

Le seguenti procedure consentono di installare un server Web Apache con supporto PHP e MariaDB (un fork di MySQL sviluppato dalla comunità) sull'istanza (a volte chiamata server web LAMP o stack LAMP). AL2 Puoi usare questo server per ospitare un sito Web statico o distribuire un'applicazione PHP dinamica che legge e scrive informazioni in un database.

> **Important**
>
> Se si sta tentando di configurare un server web LAMP su una distribuzione diversa, come Ubuntu o Red Hat Enterprise Linux, questo tutorial non funzionerà. AL2023Per, AL2023 consulta Installare un server LAMP su. Per Ubuntu, consulta la seguente documentazione

della community di Ubuntu: ApacheMySQLPHP. Per altre distribuzioni, consulta la relativa documentazione specifica.

Opzione: completare questo tutorial mediante Automation

Per completare questo tutorial utilizzando AWS Systems Manager Automation anziché le seguenti attività, esegui il AWS documento ALAMPServer Docs-Install - Automation. AL2

Processi

- Fase 1: preparare il server LAMP
- Fase 2: verificare il server LAMP
- Fase 3: proteggere il server di database
- Fase 4: (Facoltativo) Installazione phpMyAdmin
- Risoluzione dei problemi
- Argomenti correlati

Fase 1: preparare il server LAMP

Prerequisiti

- Questo tutorial presuppone che tu abbia già avviato una nuova istanza utilizzando AL2, con un nome DNS pubblico raggiungibile da Internet. Per ulteriori informazioni, consulta Launch an instance nella Amazon EC2 User Guide. È inoltre necessario aver configurato il gruppo di sicurezza per consentire le connessioni SSH (porta 22), HTTP (porta 80) e HTTPS (porta 443). Per ulteriori informazioni su questi prerequisiti, consulta le regole dei gruppi di sicurezza nella Guida per l'utente di Amazon EC2.
- La seguente procedura installa l'ultima versione di PHP attualmente disponibile su. AL2 `php8.2` Se hai in programma di utilizzare applicazioni PHP diverse da quelle descritte in questo tutorial, devi controllare che siano compatibili con `php8.2`.

Per preparare il server LAMP

1. Connettiti alla tua istanza.
2. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza. Questo processo può richiedere alcuni minuti, ma è importante

assicurarsi di disporre della versione più recente degli aggiornamenti della sicurezza e delle correzioni dei bug.

L'opzione `-y` installa gli aggiornamenti senza chiedere conferma. Se desideri esaminare gli aggiornamenti prima di installarli, puoi omettere questa opzione.

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

3. Installare i repository Amazon Linux Extras `mariadb10.5` per ottenere le versioni più recenti del pacchetto e MariaDB.

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

Se si verifica un errore indicante `sudo: amazon-linux-extras: command not found`, l'istanza non è stata avviata con un'AMI 2 di Amazon Linux (forse stai utilizzando Amazon Linux AMI). È possibile visualizzare la versione di Amazon Linux con il comando seguente.

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

4. Installa i repository `php8.2` Amazon Linux Extras per ottenere la versione più recente del PHP pacchetto per. AL2

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

5. Ora che l'istanza è corrente, è possibile installare i pacchetti del server Web Apache, MariaDB e PHP. Utilizzare il comando yum per installare contemporaneamente più pacchetti software e tutte le dipendenze correlate.

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

È possibile visualizzare le versioni correnti di tali pacchetti utilizzando il comando seguente:

```
yum info package_name
```

6. Avviare il server Web Apache.

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

7. Utilizzare il comando systemctl per configurare il server Web Apache per l'avvio a ogni avvio del sistema.

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

Puoi verificare che httpd sia attivo eseguendo il seguente comando:

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

8. Se ancora non è stato fatto, aggiungere una regola di sicurezza per consentire le connessioni HTTP (porta 80) entranti all'istanza. Per impostazione predefinita, durante l'inizializzazione è stato configurato un gruppo *N* di sicurezza launch-wizard per l'istanza. Questo gruppo contiene una regola singola per consentire connessioni SSH.

   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

   b. Scegliere Instances (Istanze) e selezionare l'istanza.

   c. Nella scheda Security (Sicurezza) visualizzare le regole in entrata. Verrà visualizzata la regola seguente:

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

> **Warning**
>
> L'utilizzo `0.0.0.0/0` consente a tutti gli IPv4 indirizzi di accedere all'istanza tramite SSH. L'opzione è accettabile per un breve periodo di tempo in un ambiente di test, ma non è sicura per gli ambienti di produzione. In produzione, potrai autorizzare solo un determinato indirizzo IP o un intervallo di indirizzi per accedere a un'istanza.

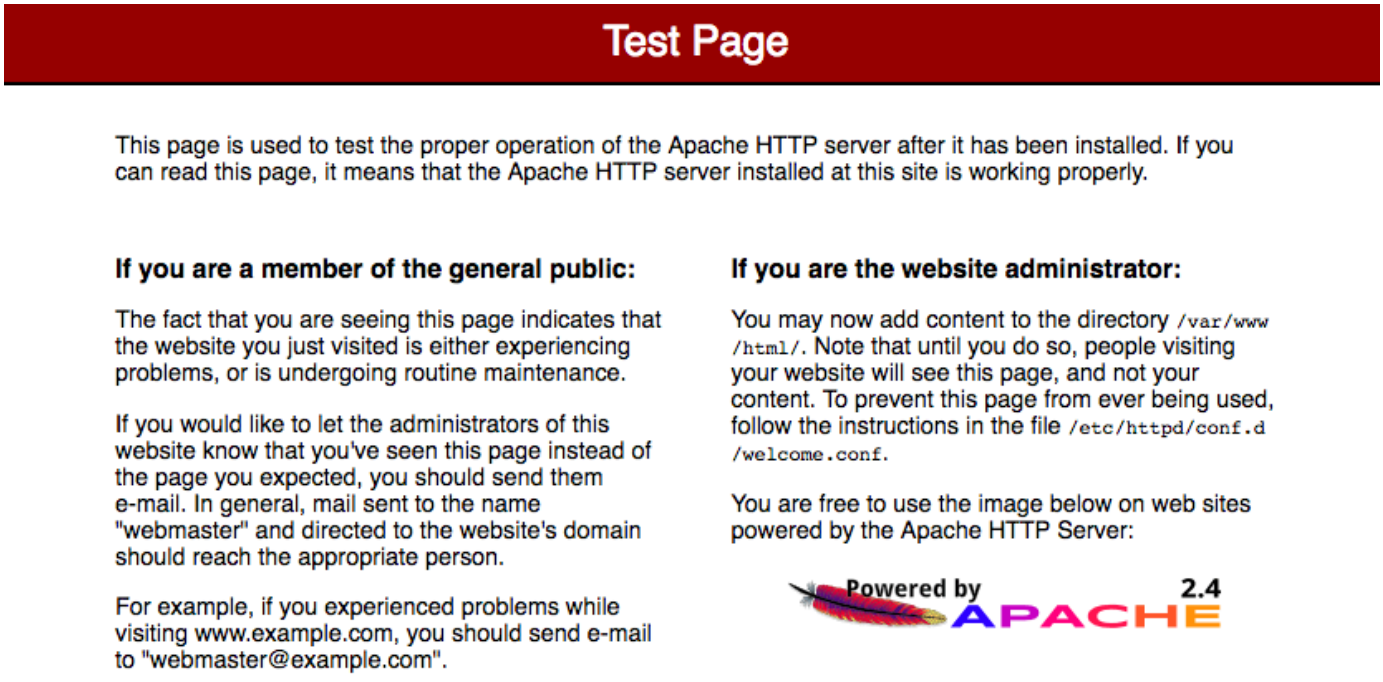
   d. Scegliere il collegamento per il gruppo di sicurezza. Utilizzando le procedure in Aggiungi regole a un gruppo di sicurezza, aggiungi una nuova regola di sicurezza in entrata con i seguenti valori:

   - Type (Tipo): HTTP
   - Protocollo: TCP
   - Port Range (Intervallo porte): 80
   - Source (Origine): personalizzata

9. Verificare il server Web. Nel browser Web, digitare l'indirizzo DNS pubblico (o l'indirizzo IP pubblico) dell'istanza. In assenza di contenuti in `/var/www/html`, dovrebbe venire visualizzata la pagina di test di Apache. È possibile ottenere il DNS pubblico per l'istanza utilizzando la console Amazon EC2 (controllare la colonna Public DNS (DNS pubblico); se la colonna è nascosta, scegliere Show/Hide Columns (Mostra/nascondi colonne) (l'icona a forma di ingranaggio) e quindi Public DNS (DNS pubblico)).

   Verificare che il gruppo di sicurezza per l'istanza contenga una regola per consentire il traffico HTTP sulla porta 80. Per ulteriori informazioni, consulta Aggiungere regole al gruppo di sicurezza.

   > **Important**
   >
   > Se non si utilizza Amazon Linux, potrebbe inoltre essere necessario configurare il firewall sull'istanza per consentire tali connessioni. Per ulteriori informazioni sulla modalità di configurazione del firewall, consulta la documentazione per la distribuzione specifica.



Apache httpd utilizza i file che sono tenuti in una directory chiamata root del documento di Apache. La root del documento di Apache Amazon Linux è `/var/www/html`, che per impostazione predefinita è di proprietà della root.

Per permettere all'account `ec2-user` di manipolare file nella directory, è necessario modificare la proprietà e le autorizzazioni della directory. Sono disponibili molti modi per completare questa attività. In questo tutorial, aggiungi l'utente `ec2-user` al gruppo `apache` per assegnare la proprietà del gruppo `apache` della directory `/var/www` e assegnare autorizzazioni di scrittura al gruppo.

Per impostare le autorizzazioni dei file

1. Aggiungere l'utente (in questo caso `ec2-user`) al gruppo `apache`.

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

2. Uscire e ripetere l'accesso per scegliere il nuovo gruppo, quindi verificare l'appartenenza.

   a. Uscire (utilizzare il comando exit o chiudere la finestra terminale):

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

   b. Per verificare l'appartenenza al gruppo `apache`, riconnettersi all'istanza, quindi eseguire il seguente comando:

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

3. Modificare la proprietà del gruppo di `/var/www` e dei suoi contenuti al gruppo `apache`.

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

4. Per aggiungere le autorizzazioni di scrittura di gruppo e impostare l'ID di gruppo nelle sottodirectory future, modificare le autorizzazioni di directory di `/var/www` e delle relative sottodirectory.

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

5. Per aggiungere le autorizzazioni di scrittura di gruppo, modificare in modo ricorsivo le autorizzazioni del file di `/var/www` e delle relative sottodirectory:

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

Ora, `ec2-user` (e qualsiasi membro futuro del gruppo `apache`) può aggiungere, eliminare e modificare i file nella root del documento di Apache, consentendoti di aggiungere contenuti, ad esempio un sito Web statico o un'applicazione PHP.

Per proteggere il server Web (facoltativo)

Un server Web che esegue il protocollo HTTP non offre alcuna sicurezza di trasporto per i dati inviati e ricevuti. Quando ti connetti a un server HTTP utilizzando un browser Web, URLs ciò che visiti, il contenuto delle pagine Web che ricevi e il contenuto (comprese le password) di tutti i moduli HTML che invii sono tutti visibili agli intercettatori ovunque lungo il percorso di rete. La best practice per la protezione del tuo server Web prevede l'installazione del supporto per HTTPS (HTTP Secure), che protegge i dati con la crittografia SSL/TLS.

Per informazioni sull'abilitazione di HTTPS sul server, consulta Tutorial: Configura SSL/TLS su AL2.

Fase 2: verificare il server LAMP

Se il server è installato e in esecuzione e le autorizzazioni dei file sono impostate correttamente, l'account `ec2-user` dovrebbe essere in grado di creare un file PHP nella directory `/var/www/html` disponibile da Internet.

Per verificare il server LAMP

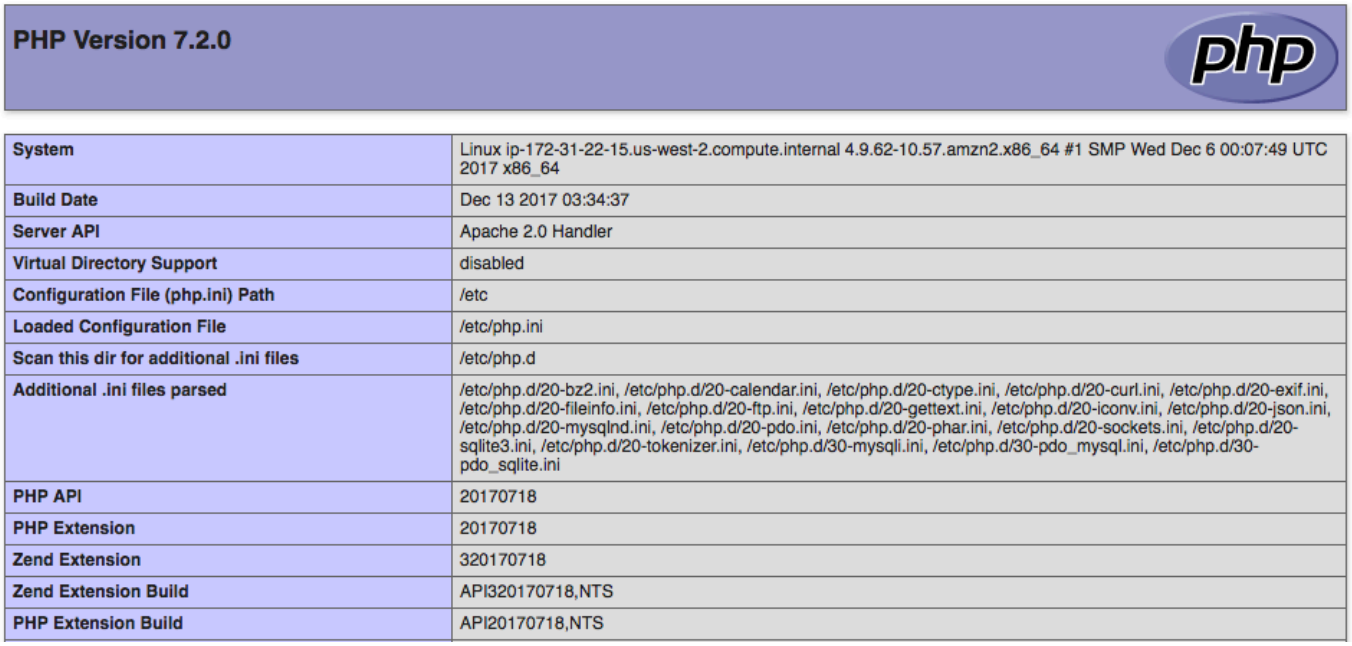
1. Creare un file PHP nella root del documento di Apache.

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

   Se si verifica un errore "Permission denied" (Autorizzazione negata) quando si tenta di eseguire questo comando, provare a uscire e accedere nuovamente per ottenere le autorizzazioni di gruppo appropriate configurate in Per impostare le autorizzazioni dei file.
2. In un browser Web, digitare l'URL del file appena creato. Questo URL è l'indirizzo DNS pubblico dell'istanza, seguito da una barra e dal nome di file. Ad esempio:

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

   Viene visualizzata la pagina delle informazioni PHP:



PHP Version 7.2.0

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

Se non viene visualizzata questa pagina, verifica che il file `/var/www/html/phpinfo.php` sia stato creato correttamente nella fase precedente. È anche possibile verificare che tutti i pacchetti richiesti siano stati installati con il seguente comando.

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

Se uno dei pacchetti richiesti non è elencato nell'output, installarlo utilizzando il comando sudo yum install ***package***. Verificare inoltre che extra `php7.2` e `lamp-mariadb10.2-php7.2` siano abilitati nell'output del comando amazon-linux-extras.

3. Eliminare il file `phpinfo.php`. Sebbene questa informazione possa essere utile, non deve essere divulgata su Internet per ragioni di sicurezza.

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

Ora si dovrebbe avere un server Web LAMP completamente funzionante. Se vengono aggiunti contenuti alla root del documento di Apache su `/var/www/html`, dovrebbe essere possibile visualizzare tali contenuti all'indirizzo DNS pubblico per l'istanza.

Fase 3: proteggere il server di database

L'installazione predefinita del server MariaDB ha diverse caratteristiche che sono ottime per test e sviluppo, ma dovrebbero essere disabilitate o rimosse per i server di produzione. Il comando

mysql_secure_installation guida attraverso il processo di impostazione di una password root e la rimozione delle caratteristiche non protette dall'installazione. Anche se non hai intenzione di utilizzare il server MariaDB, consigliamo di eseguire questa procedura.

Per proteggere il server MariaDB

1. Avviare il server MariaDB.

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

2. Esegui mysql_secure_installation.

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

   a. Quando richiesto, digitare una password per l'account root.

      i. Digitare la password root corrente. Per impostazione predefinita, l'account root non ha una password configurata. Premere Invio.

      ii. Digitare **Y** per impostare una password e digitare una password sicura due volte. Per ulteriori informazioni sulla creazione di una password sicura, vedere https://identitysafe.norton.com/password-generator/. Assicurarsi di conservare questa password in un posto sicuro.

      L'impostazione di una password root per MariaDB è solo la misura di base per la protezione del database. Quando si crea o si installa un'applicazione basata su un database, normalmente si crea un utente del servizio di database per tale applicazione per evitare di usare l'account root per ragioni diverse dall'amministrazione del database.

   b. Digitare **Y** per rimuovere gli account utente anonimi.

   c. Digitare **Y** per disabilitare l'accesso root in remoto.

   d. Digitare **Y** per rimuovere il database di test.

   e. Digitare **Y** per ricaricare le tabelle dei privilegi e salvare le modifiche.

3. (Facoltativo) Se non si ha intenzione di utilizzare immediatamente il server MariaDB, interromperlo. È possibile riavviarlo quando è di nuovo necessario.

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

4. (Facoltativo) Se si desidera che il server MariaDB si avvii a ogni avvio, digitare il seguente comando.

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

Fase 4: (Facoltativo) Installazione phpMyAdmin

phpMyAdminè uno strumento di gestione dei database basato sul Web che puoi utilizzare per visualizzare e modificare i database MySQL sulla tua istanza EC2. Segui le fasi seguenti per installare e configurare `phpMyAdmin` sull'istanza Amazon Linux.

> **Important**
>
> Non è consigliabile `phpMyAdmin` utilizzarlo per accedere a un server LAMP a meno che tu non lo abbia abilitato SSL/TLS in Apache; in caso contrario, la password dell'amministratore del database e altri dati vengono trasmessi in modo non sicuro su Internet. Per i consigli sulla sicurezza forniti dagli sviluppatori, consulta Proteggere l'installazione. phpMyAdmin Per informazioni generali sulla protezione di un server Web su un'istanza EC2, consulta Tutorial: Configura SSL/TLS su AL2.

Per installare phpMyAdmin

1. Installare le dipendenze richieste.

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

2. Riavviare Apache.

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

3. Riavviare `php-fpm`.

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

4. Andare alla root del documento di Apache in `/var/www/html`.

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

5. Seleziona un pacchetto sorgente per l'ultima phpMyAdmin versione da https://www.phpmyadmin.net/downloads. Per scaricare il file direttamente nell'istanza, copiare il link e incollarlo in un comando wget, come in questo esempio:

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

6. Creare una cartella `phpMyAdmin` in cui estrarre il pacchetto con il comando seguente.

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

7. Eliminare il *`phpMyAdmin-latest-all-languages.tar.gz`* tarball.

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

8. (Facoltativo) Se il server MySQL non è in esecuzione, avviarlo in questo momento.

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

9. In un browser Web, digita l'URL dell' phpMyAdmin installazione. Questo URL è l'indirizzo DNS pubblico (o indirizzo IP pubblico) dell'istanza seguito da una barra e dal nome della directory di installazione. Esempio:

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

   Dovresti vedere la pagina phpMyAdmin di accesso:

10. Accedi all' phpMyAdmin installazione con il nome `root` utente e la password root MySQL che hai creato in precedenza.

    L'installazione deve essere configurata prima di essere messa in funzione. Si consiglia di iniziare con la creazione manuale del file di configurazione, come segue:

    a. Per iniziare con un file di configurazione minimo, utilizza l'editor di testo preferito per creare un nuovo file e quindi copia al suo interno il contenuto di `config.sample.inc.php`.
    b. Salva il file come `config.inc.php` nella phpMyAdmin directory che contiene. `index.php`
    c. Per qualsiasi configurazione aggiuntiva, fare riferimento alle istruzioni successive alla creazione del file nella sezione Uso dello script di phpMyAdmin installazione delle istruzioni di installazione.

    Per informazioni sull'utilizzo phpMyAdmin, consultate la Guida per l'phpMyAdmin utente.

Risoluzione dei problemi

Questa sezione offre suggerimenti per la risoluzione di problemi comuni che si possono incontrare quando si configura un nuovo server LAMP.

Non riesco a connettermi al mio server utilizzando un browser Web

Esegui i controlli seguenti per verificare se il tuo server Web Apache è in esecuzione e accessibile.

- Il server Web è in esecuzione?

  Puoi verificare che httpd sia attivo eseguendo il seguente comando:

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

  Se il processo httpd non è in esecuzione, ripeti le fasi descritte in Per preparare il server LAMP.

- Il firewall è configurato correttamente?

  Verificare che il gruppo di sicurezza per l'istanza contenga una regola per consentire il traffico HTTP sulla porta 80. Per ulteriori informazioni, consulta Aggiungere regole al gruppo di sicurezza.

Non riesco a connettermi al mio server utilizzando HTTPS

Eseguire le seguenti verifiche per verificare se il server Web Apache è configurato per supportare HTTPS.

- Il server Web è configurato correttamente?

  Dopo avere installato Apache, il server è configurato per il traffico HTTP. Per supportare HTTPS, abilitare TLS sul server e installare un certificato SSL. Per informazioni, consulta Tutorial: Configura SSL/TLS su AL2.

- Il firewall è configurato correttamente?

  Verificare che il gruppo di protezione per l'istanza contenga una regola per consentire il traffico HTTPS sulla porta 443. Per ulteriori informazioni, consulta Aggiungere regole a un gruppo di sicurezza.

Argomenti correlati

Per ulteriori informazioni sul trasferimento di file sull'istanza o sull'installazione di un WordPress blog sul server Web, consulta la seguente documentazione:

- Trasferisci i file sulla tua istanza Linux utilizzando WinSCP.
- Trasferisci file su istanze Linux utilizzando un SCP client.
- Tutorial: Ospita un WordPress blog su AL2

Per ulteriori informazioni sui comandi e sul software utilizzati in questo tutorial, consulta le pagine Web seguenti:

- Server Web Apache: http://httpd.apache.org/
- Server database MariaDB: https://mariadb.org/
- Linguaggi di programmazione PHP: http://php.net/
- Il `chmod` comando: https://en.wikipedia. org/wiki/Chmod
- Il `chown` comando: https://en.wikipedia. org/wiki/Chown

Per ulteriori informazioni sulla registrazione di un nome di dominio per il server Web o sul trasferimento di un nome di dominio esistente su questo host, consulta l'articolo relativo alla creazione e alla migrazione di domini e sottodomini ad Amazon Route 53 nella Guida per lo sviluppatore di Amazon Route 53.

Tutorial: Configura SSL/TLS su AL2

Secure Layer/Transport Sockets Layer Security (SSL/TLS) creates an encrypted channel between a web server and web client that protects data in transit from being eavesdropped on. This tutorial explains how to add support manually for SSL/TLSsu un'istanza EC2 con AL2 un server web Apache). Questo tutorial presuppone che si non stia utilizzando un sistema di bilanciamento del carico (load balancer). Se si utilizza Elastic Load Balancing, è possibile scegliere di configurare l'offload SSL sul load balancer, utilizzando invece un certificato di AWS Certificate Manager.

Per motivi storici, la crittografia Web viene spesso definita semplicemente con l'acronimo SSL. Se da un lato i browser Web continuano a supportare il protocollo SSL, dall'altro il protocollo TLS, suo successore, è meno vulnerabile agli attacchi. Per impostazione predefinita, AL2 disabilita il supporto lato server per tutte le versioni di SSL. Gli organismi che si occupano degli standard di sicurezza

considerano TLS 1.0 non sicuro. TLS 1.0 e TLS 1.1 sono stati dichiarati formalmente obsoleti a marzo 2021. Le istruzioni contenute in questo tutorial si basano esclusivamente sull'abilitazione di TLS 1.2. TLS 1.3 è stato finalizzato nel 2018 ed è disponibile AL2 purché la libreria TLS sottostante (OpenSSL in questo tutorial) sia supportata e abilitata. I clienti devono supportare TLS 1.2 o versioni successive entro il 28 giugno 2023. Per ulteriori informazioni sugli standard di crittografia aggiornati, consulta RFC 7568 e RFC 8446.

Questo tutorial fa riferimento alla crittografia Web moderna semplicemente come TLS.

Important

Queste procedure sono destinate all'uso con AL2. Supponiamo anche che si stia operando su una nuova istanza Amazon EC2. Se stai cercando di configurare un'istanza EC2 che esegue una distribuzione diversa o un'istanza che esegue una versione precedente di AL2, alcune procedure di questo tutorial potrebbero non funzionare. Per Ubuntu, consulta la documentazione seguente della community: Open SSL on Ubuntu (Apri SSL su Ubuntu). Per Red Hat Enterprise Linux, consulta il seguente argomento: Setting up the Apache HTTP Web Server (Configurazione del server Web HTTP Apache). Per altre distribuzioni, consulta la relativa documentazione specifica.

Note

In alternativa, puoi utilizzare AWS Certificate Manager (ACM) for AWS Nitro enclaves, un'applicazione enclave che consente di utilizzare SSL/TLS certificati pubblici e privati con applicazioni Web e server in esecuzione su istanze Amazon EC2 con Nitro Enclaves. AWS Nitro Enclaves è una funzionalità di Amazon EC2 che consente la creazione di ambienti di elaborazione isolati per proteggere ed elaborare in modo sicuro dati altamente sensibili, come certificati e chiavi private. SSL/TLS
ACM per Nitro Enclaves funziona con nginx in esecuzione sull'istanza Amazon EC2 Linux per creare chiavi private, distribuire certificati e chiavi private e gestire i rinnovi dei certificati.
Per utilizzare ACM per Nitro Enclaves, è necessario utilizzare un'istanza Linux abilitata all'enclave.
Per ulteriori informazioni, consulta Che cos'è Nitro Enclaves? AWS e AWS Certificate Manager per Nitro Enclaves nella Guida per l'utente di Nitro Enclaves.AWS

Indice

Prerequisiti

Prima di iniziare questo tutorial, completare le procedure descritte di seguito:

- Avvia un' AL2 istanza supportata da Amazon EBS. Per ulteriori informazioni, consulta Launch an instance nella Amazon EC2 User Guide.
- Configurare i gruppi di sicurezza in modo da consentire all'istanza di accettare le connessioni sulle porte TCP seguenti:
  - SSH (porta 22)
  - HTTP (porta 80)
  - HTTPS (porta 443)

  Per ulteriori informazioni, consulta Regole del gruppo di sicurezza nella Guida per l'utente di Amazon EC2.
- Installare il server Web Apache. Per step-by-step istruzioni, consulta Tutorial: Installa un server Web LAMP su AL2. Sono necessari solo il pacchetto httpd e le relative dipendenze. Puoi pertanto ignorare le istruzioni relative a PHP e MariaDB.
- Per identificare e autenticare i siti Web, l'infrastruttura a chiave pubblica (PKI) TLS si basa su Domain Name System (DNS). Per utilizzare l'istanza EC2 per ospitare un sito Web pubblico, devi registrare un nome di dominio per il server Web o trasferire un nome di dominio esistente nell'host Amazon EC2. Per questa operazione sono disponibili numerosi servizi di registrazione di domini e hosting DNS di terze parti. In alternativa, puoi utilizzare Amazon Route 53.

Fase 1: abilitare TLS nel server

Opzione: completare questo tutorial mediante Automation

Per completare questo tutorial utilizzando AWS Systems Manager l'automazione anziché le seguenti attività, esegui il documento di automazione.

Questa procedura illustra il processo di configurazione di TLS AL2 con un certificato digitale autofirmato.

> **Note**
>
> Un certificato autofirmato è accettabile in ambienti di test, ma non in ambienti di produzione. Se esponi un certificato autofirmato in Internet, i visitatori del sito visualizzeranno avvisi di sicurezza.

Per abilitare TLS in un server

1. Connettersi all'istanza e confermare che Apache è in esecuzione.

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

   Se il valore restituito non è "enabled" ("abilitato), avviare Apache e configurarlo in modo che venga avviato all'avvio del sistema:

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

2. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza. Questo processo può richiedere alcuni minuti, ma è importante assicurarsi di disporre della versione più recente degli aggiornamenti della sicurezza e delle correzioni dei bug.

   > **Note**
   >
   > L'opzione `-y` installa gli aggiornamenti senza chiedere conferma. Se desideri esaminare gli aggiornamenti prima di installarli, puoi omettere questa opzione.

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

3. Dopo aver aggiornato l'istanza, aggiungere il supporto per TLS installando il modulo Apache `mod_ssl`.

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

L'istanza dispone ora dei file seguenti, che serviranno per configurare il server sicuro e creare un certificato per il test:

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

  File di configurazione per mod_ssl. Contiene le direttive che indicano ad Apache dove cercare le chiavi e i certificati di crittografia, le versioni del protocollo TLS da consentire e il tipo di crittografia da accettare.

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

  Script che genera un certificato X.509 autofirmato e una chiave privata per l'host del server. Questo certificato risulta utile per verificare se Apache è configurato correttamente per l'utilizzo di TLS. Non deve essere usato in ambienti di produzione poiché non garantisce l'identità. In caso contrario, attiva avvisi nei browser Web.

4. Eseguire lo script per generare un certificato dummy autofirmato e una chiave per il test.

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

Viene così generato il nuovo file `localhost.crt` nella directory `/etc/pki/tls/certs/`. Il nome di file specificato corrisponde al file predefinito assegnato nella direttiva SSLCertificateFile in `/etc/httpd/conf.d/ssl.conf`

Il file contiene sia un certificato autofirmato che la relativa chiave privata. Apache richiede che certificato e chiave siano entrambi in formato PEM, che è composto da caratteri ASCII con codifica Base64 racchiusi tra le righe "BEGIN" ed "END", come nell'esempio abbreviato riportato di seguito.

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

I nomi e le estensioni di file rappresentano una convenzione e non hanno alcuna ripercussione sulla funzionalità. Ad esempio è possibile denominare un certificato `cert.crt`, `cert.pem` o con qualsiasi altro nome di file, a condizione che la direttiva corrispondente nel file `ssl.conf` utilizzi lo stesso nome.

> **Note**
>
> Quando si sostituiscono i file TLS predefiniti con file personalizzati, assicurarsi che siano in formato PEM.

5. Apri il file `/etc/httpd/conf.d/ssl.conf` utilizzando un editor di testo (come vim o nano) in qualità di utente root e commenta la riga seguente, in quanto il certificato dummy autofirmato contiene anche la chiave. Se non si commenta questa riga prima di completare il passaggio successivo, l'avvio del servizio Apache non riesce.

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

6. Riavviare Apache.

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

> **Note**
>
> Assicurarsi che la porta TCP 443 sia accessibile sull'istanza EC2, come descritto in precedenza.

7. Il server Web Apache ora dovrebbe supportare HTTPS (HTTP protetto) sulla porta 443. Per eseguire il test, digitare l'indirizzo IP o il nome di dominio completo dell'istanza EC2 nella barra degli indirizzi URL di un browser con il prefisso **`https://`**.

   Poiché ti stai connettendo a un sito con un certificato host autofirmato non attendibile, il browser potrebbe visualizzare una serie di avvisi di sicurezza. Ignorare gli avvisi e passare al sito.

   Se la pagina predefinita di test di Apache viene visualizzata, significa che TLS è stato correttamente configurato sul server. Tutti i dati in transito tra il browser e il server ora sono crittografati.

   > **Note**
   >
   > Per evitare che i visitatori del sito vedano schermate di avviso, è necessario ottenere un certificato attendibile che non solo esegua la crittografia, ma che fornisca anche un'autenticazione pubblica del proprietario del sito.

Fase 2: ottenere un certificato firmato dalla CA

Puoi utilizzare la seguente procedura per ottenere un certificato firmato dalla CA:

- Generare una richiesta di firma del certificato (CSR) da una chiave privata
- Inviare il CSR alla Certificate Authority
- Ottenere un certificato host firmato
- Configurare Apache per utilizzare il certificato

Dal punto di vista della crittografia un certificato host TLS X.509 autofirmato è identico a un certificato firmato da una CA. La differenza è una questione di attendibilità. Una CA si impegna infatti a fornire una convalida minima della titolarità di un dominio prima di emettere un certificato a un richiedente. Ogni browser Web contiene un elenco di quelli CAs ritenuti idonei dal fornitore del browser a tale scopo. Un certificato X.509 è principalmente composto da una chiave server privata e da una firma fornita dalla CA e associata a livello di crittografia alla chiave pubblica. Quando un browser si connette a un server Web tramite HTTPS, il server presenta un certificato da confrontare con l'elenco dei siti attendibili CAs. Se il firmatario è incluso nell'elenco oppure è accessibile tramite una catena di attendibilità composta da altri firmatari fidati, il browser negozia un canale di dati a crittografia rapida con il server e carica la pagina.

I certificati in genere costano poiché il processo di convalida delle richieste prevede alcuni costi. Consigliamo pertanto di valutare le varie offerte. Alcuni CAs offrono certificati di livello base gratuiti. Il più importante di questi CAs è il progetto Let's Encrypt, che supporta anche l'automazione del processo di creazione e rinnovo dei certificati. Per ulteriori informazioni sull'utilizzo di un certificato Let's Encrypt, consulta la pagina Ottenimento di Certbot.

Se hai intenzione di offrire servizi di livello commerciale, AWS Certificate Manager è una buona opzione.

L'uso di un certificato host sottostante rappresenta la soluzione ideale. Dal 2019, gruppi appartenenti alla pubblica amministrazione e a settori specifici consigliano una dimensione (modulo) di chiave minima pari a 2048 bit per le chiavi RSA a protezione dei documenti fino al 2030. La dimensione predefinita del modulo generato da OpenSSL AL2 in è di 2048 bit, adatta per l'uso in un certificato firmato da un'autorità di certificazione. Nella seguente procedura viene offerto un passaggio opzionale per coloro che desiderano una chiave personalizzata, ad esempio, una chiave con un modulo più grande o che utilizza un algoritmo di crittografia diverso.

> **Important**
>
> In mancanza di un dominio DNS registrato e ospitato, tali istruzioni per l'acquisizione di certificati host firmati dalla CA non funzioneranno.

Per ottenere un certificato firmato dalla CA

1. Connect alla propria istanza e accedi a/etc/pki/tls/private/. Si tratta della directory in cui viene memorizzata la chiave privata del server per TLS. Se preferisci utilizzare una chiave host esistente per generare la CSR, passa alla Fase 3.
2. (Opzionale) Generare una nuova chiave privata. Di seguito sono riportate alcune configurazioni di chiave di esempio. Qualsiasi chiave risultante funziona con il server Web, ma il livello e il tipo di sicurezza implementati possono variare.

   - Esempio 1: creare una chiave host RSA predefinita. Il file risultante, **`custom.key`**, è una chiave privata RSA a 2048 bit.

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

   - Esempio 2: creare una chiave RSA più complessa con un modulo più grande, Il file risultante, **`custom.key`**, è una chiave privata RSA a 4096 bit.

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

- Esempio 3: creare una chiave RSA crittografata a 4096 bit con protezione con password. Il file risultante, **`custom.key`**, è una chiave privata RSA a 4096 bit crittografata in base allo standard AES-128.

  > **Important**
  >
  > La crittografia di una chiave fornisce maggiore sicurezza, ma dal momento che una chiave crittografata richiede una password, i servizi che dipendono da essa non possono essere avviati automaticamente. Ogni volta che usi questa chiave, devi fornire la password (nell'esempio precedente, "abcde12345") tramite una connessione SSH.

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

- Esempio 4: creare una chiave utilizzando uno standard non RSA. La crittografia RSA può essere relativamente lenta per via della dimensione delle chiavi pubbliche, che sono basate sul prodotto di due grandi numeri primi. Tuttavia, è possibile creare chiavi per TLS che utilizzano una crittografia non RSA. Le chiavi basate su calcoli matematici di curve ellittiche sono di dimensioni inferiori e, dal punto di vista del calcolo, più rapide pur garantendo un livello equivalente di sicurezza.

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

  Il risultato è una chiave privata basata su curva ellittica a 256 bit che utilizza prime256v1, una "curva denominata" supportata da OpenSSL. La complessità dal punto di vista crittografico è leggermente superiore rispetto una chiave RSA a 2048 bit, secondo i dati NIST.

  > **Note**
  >
  > Non tutti CAs forniscono lo stesso livello di supporto per elliptic-curve-based le chiavi come per le chiavi RSA.

Assicurati che la nuova chiave privata abbia proprietà e autorizzazioni estremamente restrittive (owner=root, group=root, solo per il proprietario). read/write Il comando è come mostrato nell'esempio seguente.

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

I comandi precedenti restituiscono il seguente risultato:

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

Dopo aver creato e configurato una chiave affidabile, puoi creare una CSR.

3. Creare una CSR utilizzando la chiave preferita. Nell'esempio seguente viene utilizzato **`custom.key`**.

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

OpenSSL visualizza una finestra di dialogo e richiede l'immissione delle informazioni riportate nella seguente tabella. Tutti i campi, tranne Common Name (Nome comune), sono facoltativi per un certificato host di base convalidato a livello di dominio.

Nome	Descrizione	Esempio
Nome paese	L'abbreviazione ISO di due lettere per il tuo paese.	US = Stati Uniti
State or Province Name (Nome stato o provincia)	Il nome dello stato o della provincia in cui si trova la tua organizzazione. Questo nome non può essere abbreviato.	Washington
Locality Name	La località in cui si trova la tua organizza zione, ad esempio una città.	Seattle

Nome	Descrizione	Esempio
(Nome località)		
Nome organizzazione	La denominazione legale completa della tua organizzazione. Non abbreviare il nome dell'organizzazione.	Example Corporation
Organizational Unit Name (Nome unità organizzativa)	Eventuali informazioni aggiuntive.	Example Dept
Common Name (Nome comune)	Questo valore deve corrispondere esattamente all'indirizzo Web che presumibilmente gli utenti immettono in un browser. In genere, ciò significa un nome di dominio con un nome host o alias con un prefisso, nel formato **`www.example.com`** . Nei test con un certificato autofirmato e senza risoluzione DNS, il nome comune può essere costituito solo dal nome host. CAs offrono anche certificati più costosi che accettano nomi wild-card come. **`*.example.com`**	www.example.com
Indirizzo e-mail	L'indirizzo e-mail dell'amministratore del server.	someone@example.com

Infine, OpenSSL richiede l'immissione di una password di verifica opzionale. Questa password è valida solo per la CSR e per le transazioni tra te e la CA. Pertanto, attieniti alle raccomandazioni della CA in merito alla definizione di questo tipo di password e all'altro campo facoltativo, ovvero il nome azienda facoltativo. La password di verifica associata alla CSR non ha alcuna ripercussione sulla funzionalità del server.

Il file **csr.pem** risultante contiene la chiave pubblica, la firma digitale della chiave pubblica e i metadati immessi.

4. Inviare la CSR a una CA. In genere, questa operazione prevede l'apertura del file CSR in un editor di testo e la copia del contenuto in un modulo Web. In questo momento, è possibile che ti venga chiesto di fornire uno o più nomi alternativi del soggetto (SANs) da inserire nel certificato. Se **www.example.com** è il nome comune, **example.com** potrebbe essere un nome alternativo di oggetto (SAN) valido e viceversa. Un visitatore del sito che immettesse uno di questi due nomi avrebbe accesso a una connessione priva di errori. Se il modulo web CA lo consente, includi il nome comune nell'elenco di SANs. Alcuni lo CAs includono automaticamente.

   Dopo l'approvazione della richiesta, riceverai un nuovo certificato host firmato dalla CA. Ti potrebbe inoltre venire richiesto di scaricare un file di certificato intermedio contenente i certificati aggiuntivi necessari per completare la catena di attendibilità della CA.

   > **Note**
   >
   > La CA potrebbe inviare i file in più formati, destinati a scopi specifici. Ai fini di questo tutorial, ti consigliamo di usare solo un file di certificato in formato PEM, che in genere, ma non sempre, è contrassegnato dall'estensione `.pem` o `.crt`. Se non sei sicuro di quale file usare, apri il file in un editor di testo e cerca quello contenente uno o più blocchi che iniziano con la seguente riga.
   >
   > ```
   > - - - - -BEGIN CERTIFICATE - - - - -
   > ```
   >
   > Il file deve inoltre terminare con la seguente riga.
   >
   > ```
   > - - - -END CERTIFICATE - - - - -
   > ```
   >
   > Puoi anche testare il file nella riga di comando come indicato di seguito.
   >
   > ```
   > [ec2-user certs]$ openssl x509 -in certificate.crt -text
   > ```
   >
   > Verifica che nel file appaiano queste righe. Non utilizzare file che terminano con `.p7b`, `.p7c` o estensioni simili.

5. Posizionare il nuovo certificato firmato dalla CA ed eventuali certificati intermedi nella directory `/etc/pki/tls/certs`.

> **Note**
>
> Esistono vari modi per caricare il nuovo certificato nell'istanza EC2, ma il più semplice e immediato prevede di aprire un editor di testo (ad esempio, vi, nano o notepad) sul computer locale e sull'istanza e quindi di copiare e incollare il contenuto del file in queste posizioni. Devi disporre delle autorizzazioni root [sudo] durante l'esecuzione di queste operazioni nell'istanza EC2. In questo modo, puoi verificare in tempo reale se si verificano problemi a livello di autorizzazioni o percorsi. Presta particolare attenzione a non aggiungere altre righe durante la copia del contenuto o a non apportare modifiche di alcun tipo.

Dall'interno della `/etc/pki/tls/certs` directory, verifica che le impostazioni di proprietà del file, gruppo e autorizzazione corrispondano ai AL2 valori predefiniti altamente restrittivi (owner=root, group=root, solo per il proprietario). read/write L'esempio seguente mostra i comandi da utilizzare.

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

Questi comandi dovrebbero restituire il seguente risultato.

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

Le autorizzazioni del file del certificato intermedio sono meno rigide (owner=root, group=root, il proprietario può scrivere, il gruppo può leggere, tutti gli utenti possono leggere). L'esempio seguente mostra i comandi da utilizzare.

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

Questi comandi dovrebbero restituire il seguente risultato.

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

6. Posizionare la chiave privata utilizzata per creare la CRS nella directory `/etc/pki/tls/private/`.

   > **Note**
   >
   > Esistono vari modi per caricare la chiave personalizzata nell'istanza EC2, ma il più semplice e immediato prevede di aprire un editor di testo (ad esempio, vi, nano o notepad) sul computer locale e sull'istanza e quindi di copiare e incollare il contenuto del file in queste posizioni. Devi disporre delle autorizzazioni root [sudo] durante l'esecuzione di queste operazioni nell'istanza EC2. In questo modo, puoi verificare in tempo reale se si verificano problemi a livello di autorizzazioni o percorsi. Presta particolare attenzione a non aggiungere altre righe durante la copia del contenuto o a non apportare modifiche di alcun tipo.

   Dall'interno della `/etc/pki/tls/private` directory, usa i seguenti comandi per verificare che le impostazioni di proprietà, gruppo e autorizzazione dei file corrispondano ai valori AL2 predefiniti altamente restrittivi (owner=root, group=root, solo per il proprietario). 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
   ```

   Questi comandi dovrebbero restituire il seguente risultato.

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

7. Modificare `/etc/httpd/conf.d/ssl.conf` per riflettere i nuovi file del certificato e della chiave.

   a. Indicare il percorso e il nome del file del certificato host firmato dalla CA nella direttiva `SSLCertificateFile` di Apache:

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

   b. In caso di ricezione di un file del certificato intermedio (`intermediate.crt` in questo esempio), specificare il relativo percorso e nome di file utilizzando la direttiva `SSLCACertificateFile` di Apache:

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

> **Note**
>
> Alcuni CAs combinano il certificato host e i certificati intermedi in un unico file, rendendo la direttiva non necessaria. `SSLCACertificateFile` Consultare le istruzioni fornite dalla CA.

c. Specificare il percorso e il nome del file della chiave privata (`custom.key` in questo esempio) nella direttiva `SSLCertificateKeyFile` di Apache:

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

8. Salvare `/etc/httpd/conf.d/ssl.conf` e riavviare Apache.

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

9. Testare il server digitando il nome del dominio nella barra dell'URL di un browser con il prefisso `https://`. Il browser deve caricare la pagina di test su HTTPS senza errori.

Fase 3: testare e proteggere la configurazione di sicurezza

Dopo aver configurato TLS e averlo esposto al pubblico, devi testarne il livello effettivo di sicurezza. Questa operazione è semplice grazie a servizi online quali Qualys SSL Labs, che eseguono un'analisi completa e gratuita della configurazione della sicurezza. In base ai risultati, puoi decidere di rafforzare la configurazione di sicurezza di default mediante il controllo dei protocolli accettati, del tipo di cifratura preferito e degli elementi da escludere. Per ulteriori informazioni, consulta la sezione relativa alla formulazione delle classificazioni di Qualys.

> **Important**
>
> Il test in un ambiente reale è di cruciale importanza per la sicurezza del server. Piccoli errori di configurazione potrebbero generare gravi violazioni della sicurezza e perdita di dati. Poiché le procedure consigliate per la sicurezza sono in costante cambiamento in risposta a programmi di ricerca e minacce emergenti, verifiche periodiche della sicurezza rappresentano una pratica di amministrazione ottimale dei server.

Nel sito Qualys SSL Labs, immetti il nome di dominio completo del server nel formato **`www.example.com`**. Dopo circa due minuti riceverai una valutazione del sito (da A a F) e un'analisi dettagliata dei risultati. La tabella seguente riassume il rapporto per un dominio con impostazioni identiche alla configurazione predefinita di Apache e con un certificato Certbot predefinito. AL2

Valutazione complessiva	B
Certificato	100%
Supporto dei protocolli	95%
Scambio di chiavi	70%
Affidabilità crittografia	90%

Benché dalla panoramica emerga una certa solidità della configurazione, il rapporto dettagliato mette in luce diversi potenziali problemi, qui elencati in ordine di gravità:

✗ La RC4 crittografia è supportata per l'uso da parte di alcuni browser meno recenti. Un codice è il nucleo matematico di un algoritmo di crittografia. RC4, un codice veloce utilizzato per crittografare i flussi di dati TLS, è noto per presentare diversi gravi punti deboli. A meno di avere ottime ragioni per supportare browser legacy, è necessario disabilitare questa opzione.

✗ Sono supportate versioni di TLS meno recenti. La configurazione supporta TLS 1.0 (già obsoleto) e TLS 1.1 (in procinto di diventare obsoleto). A partire dal 2018, è raccomandato soltanto TLS 1.2.

✗ La proprietà Forward Secrecy non è completamente supportata. La proprietà Forward Secrecy è una caratteristica degli algoritmi che eseguono la crittografia utilizzando chiavi di sessione temporanee (effimere) derivate dalla chiave privata. Ciò in pratica significa che gli utenti malintenzionati non possono decriptare i dati HTTPS anche se sono in possesso della chiave privata a lungo termine di un server Web.

Per correggere e rendere valida anche per il futuro la configurazione TLS

1. Aprire il file di configurazione `/etc/httpd/conf.d/ssl.conf` in un editor di testo e commentare la seguente riga inserendo il carattere "#" all'inizio:

   ```
   #SSLProtocol all -SSLv3
   ```

2. Aggiungere la seguente direttiva:

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

Questa direttiva disabilita in modo esplicito SSL versioni 2 e 3, nonché TLS versioni 1.0 e 1.1. Il server ora non accetta più connessioni crittografate con client che utilizzano crittografie diverse da TLS 1.2. Le descrizioni dettagliate della direttiva illustrano più chiaramente al lettore la tipologia di configurazione impostata per il server.

> **Note**
>
> La disabilitazione di TLS versioni 1.0 e 1.1 consente di bloccare l'accesso al sito da parte di una piccola percentuale di browser Web non aggiornati.

Per modificare l'elenco delle crittografie consentite

1. Nel file di configurazione `/etc/httpd/conf.d/ssl.conf`, individuare la sezione con la direttiva **`SSLCipherSuite`** e commentare la riga esistente inserendo il carattere "#" all'inizio.

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

2. Specificare suite di crittografia esplicite e un ordine di crittografia che dia priorità alla funzione Forward Secrecy e che eviti crittografie non sicure. La direttiva `SSLCipherSuite` qui utilizzata si basa su un output del generatore di configurazioni SSL di Mozilla, che personalizza una configurazione TLS in funzione del software specifico in esecuzione sul server Per prima cosa determinare le versioni di Apache e OpenSSL in base all'output dei seguenti comandi.

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

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

Ad esempio, se l'informazione restituita è Apache 2.4.34 e OpenSSL 1.0.2, inserirla nel generatore. Scegliere poi il modello di compatibilità “moderna”, che crea una direttiva `SSLCipherSuite` e applica in modo rigido la sicurezza ma che funziona per la maggior parte dei browser. Se il software non supporta la configurazione moderna, è possibile aggiornarlo o scegliere la configurazione “intermedia”.

```
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
```

Le crittografie selezionate includono nel proprio nome l'acronimo ECDHE (, abbreviazione di Elliptic Curve Diffie-Hellman Ephemeral). Il termine effimero fa riferimento alla proprietà Forward Secrecy. Come sottoprodotto, questi codici non supportano. RC4

È consigliabile utilizzare un elenco esplicito di crittografie anziché utilizzare le impostazioni predefinite o le direttive concise il cui contenuto non è visibile.

Copiare la direttiva generata in `/etc/httpd/conf.d/ssl.conf`.

> **Note**
>
> Nonostante in questa sede siano riportate su più righe per facilitarne la leggibilità, una volta copiata su `/etc/httpd/conf.d/ssl.conf` la direttiva deve trovarsi su un'unica riga con solo due punti (senza spazi) tra i nomi di crittografia.

3. Rimuovere infine i commenti mediante la rimozione del carattere "#" dall'inizio della riga:

```
#SSLHonorCipherOrder on
```

Questa direttiva obbliga il server a preferire crittografie con classificazione più elevata, comprese (in questo caso) quelle che supportano la proprietà Forward Secrecy. Con questa direttiva abilitata, il server cerca di stabilire una connessione stabile e affidabile prima di ripiegare sulle crittografie consentite con un livello inferiore di sicurezza.

Dopo aver completato entrambe le procedure, salvare le modifiche a `/etc/httpd/conf.d/ssl.conf` e riavviare Apache.

Se testate nuovamente il dominio su Qualys SSL Labs, dovreste vedere che la RC4 vulnerabilità e gli altri avvisi sono scomparsi e il riepilogo sarà simile al seguente.

Valutazione complessiva	A
Certificato	100%
Supporto dei protocolli	100%
Scambio di chiavi	90%
Affidabilità crittografia	90%

Ogni aggiornamento a OpenSSL introduce nuove crittografie e rimuove il supporto per quelle vecchie. Conserva la tua AL2 istanza EC2 up-to-date, tieni d'occhio gli annunci sulla sicurezza di OpenSSL e fai attenzione alle segnalazioni di nuovi exploit di sicurezza pubblicate dalla stampa tecnica.

Risoluzione dei problemi

- Il server Web Apache non si avvia a meno che non venga fornita una password

  Si tratta del comportamento previsto se per il server hai installato una chiave privata crittografata e protetta con password.

  Puoi rimuovere i requisiti di crittografia e password dalla chiave. Supponiamo, ad esempio, di avere una chiave RSA crittografata privata denominata `custom.key` nella directory di default e associata alla password **`abcde12345`**. Per generare una versione non crittografata della chiave, devi eseguire i seguenti comandi nell'istanza EC2:

  ```
  [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
  ```

  A questo punto, Apache viene avviato senza visualizzare alcuna richiesta di password.

- Vengono visualizzati errori quando eseguo il comando sudo yum install -y mod_ssl.

Quando installi i pacchetti richiesti per SSL, è possibile che vengano visualizzati errori simili ai seguenti.

```
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
```

Ciò significa in genere che l'istanza EC2 non è in esecuzione. AL2 Questo tutorial supporta solo istanze appena create a partire da un'AMI di AL2 ufficiale.

Tutorial: Ospita un WordPress blog su AL2

Le seguenti procedure ti aiuteranno a installare, configurare e proteggere un WordPress blog sulla tua istanza AL2. Questo tutorial è una buona introduzione all'uso di Amazon EC2 in quanto hai il pieno controllo su un server Web che ospita il tuo WordPress blog, cosa non tipica di un servizio di hosting tradizionale.

È tua responsabilità aggiornare i pacchetti software e gestire le patch di sicurezza del server. Per un' WordPress installazione più automatizzata che non richieda l'interazione diretta con la configurazione del server Web, il CloudFormation servizio fornisce un WordPress modello che può anche aiutarti a iniziare rapidamente. Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS CloudFormation . Se hai bisogno di una soluzione ad alta disponibilità con un database disaccoppiato, consulta Implementazione di un WordPress sito Web ad alta disponibilità nella Guida per gli sviluppatori.AWS Elastic Beanstalk

> **Important**
>
> Queste procedure sono destinate all'uso con. AL2 Per ulteriori informazioni su altre distribuzioni, consulta la documentazione specifica. Numerose fasi in questo tutorial non funzionano sulle istanze Ubuntu. Per informazioni WordPress sull'installazione su un'istanza di Ubuntu, WordPressconsulta la documentazione di Ubuntu. Puoi anche CodeDeployutilizzarlo per eseguire questa operazione su sistemi Amazon Linux, macOS o Unix.

Argomenti

- Prerequisiti

Prerequisiti

Questo tutorial presuppone che tu abbia avviato un' AL2 istanza con un server web funzionale con PHP e supporto per database (MySQL o MariadB) seguendo tutti i passaggi indicati. Tutorial: installa un server LAMP su AL2 Questo tutorial include inoltre la procedura per configurare un gruppo di sicurezza che consenta il traffico HTTP e HTTPS, nonché varie fasi da eseguire per verificare che le autorizzazioni di file siano state configurate correttamente per il server Web. Per informazioni sull'aggiunta di regole al gruppo di sicurezza, consulta Aggiungere regole a un gruppo di sicurezza.

Ti consigliamo vivamente di associare un indirizzo IP elastico (EIP) all'istanza che stai utilizzando per ospitare un WordPress blog. Ciò impedisce all'indirizzo DNS pubblico dell'istanza di modificare e interrompere l'installazione. Se sei proprietario di un nome di dominio e vuoi utilizzarlo per il tuo blog, puoi aggiornare il record DNS del nome di dominio in modo che punti all'indirizzo EIP (per ulteriori informazioni su questa procedura, contatta il registrar di nomi di dominio). Puoi usufruire di un indirizzo EIP associato a un'istanza in esecuzione gratuitamente. Per ulteriori informazioni, consulta Indirizzi IP elastici nella Guida per l'utente di Amazon EC2.

Se non disponi ancora di un nome di dominio per il tuo blog, puoi registrare un nome di dominio con Route 53 e associare l'indirizzo EIP dell'istanza al nome di dominio. Per ulteriori informazioni, consulta la pagina relativa alla registrazione dei nomi di dominio utilizzando Amazon Route 53 nella Guida per lo sviluppatore di Amazon Route 53.

Installa WordPress

Opzione: completare questo tutorial mediante Automation

Per completare questo tutorial utilizzando AWS Systems Manager l'automazione anziché le seguenti attività, esegui il documento di automazione.

Connect all'istanza e scarica il pacchetto WordPress di installazione.

Per scaricare e decomprimere il pacchetto di WordPress installazione

1. Scarica il pacchetto di WordPress installazione più recente con il wget comando. Il comando seguente dovrebbe scaricare sempre la versione più recente.

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

2. Decomprimere ed estrarre il pacchetto di installazione. La cartella di installazione viene decompressa in una cartella denominata `wordpress`.

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

Per creare un utente del database e un database per l' WordPress installazione

WordPress L'installazione deve archiviare informazioni, come post di blog e commenti degli utenti, in un database. Questa procedura consente di creare un database del blog e un utente autorizzato a leggere e salvare le informazioni in tale database.

1. Avviare il server di database.
   -
```
[ec2-user ~]$ sudo systemctl start mariadb
```
2. Accedere al server di database come utente `root`. Immetti la password database `root` quando viene richiesto. Questa password potrebbe essere diversa dalla password del sistema `root` oppure potrebbe anche essere vuota se non hai impostato alcuna protezione per il server di database.

   Se non hai ancora definito la protezione del server di database, è importante che tu lo faccia ora. Per ulteriori informazioni, vedere Per proteggere il server MariaDB (AL2).

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

3. Creare un utente e una password per il database MySQL. L' WordPressinstallazione utilizza questi valori per comunicare con il database MySQL.

   Assicurarsi di creare una password complessa per l'utente. Non utilizzare l'apostrofo (') nella password perché interromperebbe l'esecuzione del comando che lo precede. Non riutilizzare una password esistente e accertarsi di memorizzare questa password in un luogo sicuro.

   Immettere il seguente comando, ricordandosi di sostituire gli argomenti con un nome utente univoco e una password.

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

4. Creare il database. Assegnare al database un nome descrittivo e significativo, ad esempio `wordpress-db`.

   > **Note**
   >
   > I segni di punteggiatura che racchiudono il nome del database nel comando riportato di seguito sono definiti backtick (apice retroverso). Il tasto del segno backtick (apice retroverso) (`) in genere si trova sopra il tasto Tab su una tastiera standard. I backtick non sono sempre richiesti, ma consentono di utilizzare caratteri altrimenti non validi, ad esempio i trattini, nei nomi di database.

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

5. Concedi i privilegi completi per il tuo database all' WordPress utente che hai creato in precedenza.

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

6. Scaricare i privilegi del database per implementare tutte le modifiche apportate.

   ```
   FLUSH PRIVILEGES;
   ```

7. Uscire dal client `mysql`.

   ```
   exit
   ```

Per creare e modificare il file wp-config.php

La cartella WordPress di installazione contiene un file di configurazione di esempio chiamato`wp-config-sample.php`. In questa procedura, puoi copiare questo file e modificarlo in modo conforme a una configurazione specifica.

1. Copiare il file `wp-config-sample.php` in un file denominato `wp-config.php`. In questo modo, crei un nuovo file di configurazione mantenendo intatto il file campione originale come backup.

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

2. Modificare il file `wp-config.php` con l'editor di testo preferito (ad esempio nano o vim) e immettere i valori dell'installazione in uso. Se non si dispone di un editor di testo preferito, `nano` è adatto agli utenti non esperti.

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

   a. Cercare la riga che definisce `DB_NAME` e modificare `database_name_here` utilizzando il nome di database creato in Step 4 di Per creare un utente del database e un database per l' WordPress installazione.

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

   b. Cercare la riga che definisce `DB_USER` e modificare `username_here` utilizzando l'utente database creato in Step 3 di Per creare un utente del database e un database per l' WordPress installazione.

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

   c. Cercare la riga che definisce `DB_PASSWORD` e modificare `password_here` utilizzando la password complessa creata in Step 3 di Per creare un utente del database e un database per l' WordPress installazione.

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

   d. Cercare la sezione denominata `Authentication Unique Keys and Salts`. Questi `KEY` e questi `SALT` valori forniscono un livello di crittografia ai cookie del browser che WordPress gli utenti archiviano sui loro computer locali. In sostanza, l'aggiunta di valori lunghi e casuali rende il sito più sicuro. Visita https://api.wordpress. org/secret-key/1.1/salt/ per generare in modo casuale un set di valori chiave che puoi copiare e incollare nel tuo `wp-config.php` file. Per incollare il testo in un'applicazione terminale PuTTY, posizionare il cursore nel punto in cui si desidera incollare il teste e fare clic con il pulsante destro del mouse all'interno dell'applicazione terminale PuTTY.

      Per ulteriori informazioni sulle chiavi di sicurezza, visita https://wordpress. org/support/article/editing-wp-config-php/#security -keys.

> **Note**
>
> I valori riportati di seguito sono a solo scopo di esempio. Non utilizzarli per l'installazione in uso.

```
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. Salva il file ed esci dall'editor di testo.

Per installare i WordPress file nella cartella principale del documento Apache

- Dopo aver decompresso la cartella di installazione, creato un database e un utente MySQL e personalizzato il file di WordPress configurazione, è possibile copiare i file di installazione nella cartella principale dei documenti del server Web in modo da poter eseguire lo script di installazione che completa l'installazione. La posizione di questi file dipende dal fatto che il WordPress blog sia disponibile nella directory principale effettiva del server Web (ad esempio,*my.public.dns.amazonaws.com*) o in una sottodirectory o cartella sotto la radice (ad esempio,*my.public.dns.amazonaws.com/blog*).
  - Se volete WordPress eseguirlo dalla cartella principale del documento, copiate il contenuto della directory di installazione di wordpress (ma non la directory stessa) come segue:

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

- Se volete WordPress eseguirlo in una directory alternativa sotto la radice del documento, create prima quella directory e poi copiate i file al suo interno. In questo esempio, WordPress verrà eseguito dalla directory`blog`:

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

> **Important**
>
> Per motivi di sicurezza, se non si passa immediatamente alla procedura successiva, arrestare ora il server Web Apache (`httpd`). Dopo aver spostato l'installazione nella directory principale del documento Apache, lo script di WordPress installazione non è protetto e un utente malintenzionato potrebbe accedere al tuo blog se il server web Apache fosse in esecuzione. Per arrestare il server Web Apache, immettere il comando sudo systemctl stop httpd. Se invece si passa alla procedura successiva, non è necessario arrestare il server Web Apache.

Per consentire l'uso dei permalink WordPress

WordPress i permalink devono utilizzare i `.htaccess` file Apache per funzionare correttamente, ma questo non è abilitato di default su Amazon Linux. Utilizza la seguente procedura per consentire tutte le modifiche nella directory radice dei documenti di Apache.

1. Aprire il file `httpd.conf` con l'editor di testo preferito (ad esempio nano o vim). Se non si dispone di un editor di testo preferito, `nano` è adatto agli utenti non esperti.

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

2. Cercare la sezione che inizia con `<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. Modificare la riga `AllowOverride None` nella sezione precedente in modo che sia impostata nel seguente modo: `AllowOverride All`.

> **Note**
>
> Sono presenti più righe `AllowOverride` in questo file. Assicurarsi di modificare la riga nella sezione `<Directory "/var/www/html">`.

```
AllowOverride All
```

4. Salva il file ed esci dall'editor di testo.

Per installare la libreria di disegni grafici PHP su AL2

La libreria GD per PHP consente di modificare le immagini. Installa questa libreria se hai bisogno di ritagliare l'immagine di intestazione per il tuo blog. La versione da installare potrebbe richiedere una versione minima specifica di questa libreria (ad esempio, la versione 7.2). phpMyAdmin

Usa il seguente comando per installare la libreria di disegni grafici PHP su. AL2 Ad esempio, se hai installato php7.2 da amazon-linux-extras come parte dell'installazione dello stack LAMP, questo comando installa la versione 7.2 della libreria di disegni grafici PHP.

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

Per verificare la versione installata utilizza il seguente comando:

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

Di seguito è riportato un output di esempio:

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

Per correggere le autorizzazioni di file sul server Web Apache

Alcune delle funzionalità disponibili WordPress richiedono l'accesso in scrittura alla radice del documento Apache (come il caricamento di contenuti multimediali tramite le schermate di amministrazione). Se non l'avete ancora fatto, applicate le seguenti appartenenze ai gruppi e autorizzazioni (come descritto più dettagliatamente nella). Tutorial: installa un server LAMP su AL2

1. Garantire la proprietà dei file di `/var/www` e dei suoi contenuti all'utente `apache`.

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

2. Garantire la proprietà del gruppo di `/var/www` e dei suoi contenuti al gruppo `apache`.

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

3. Modificare le autorizzazioni a livello di directory di `/var/www` e delle relative sottodirectory per aggiungere le autorizzazioni di scrittura e impostare l'ID gruppo per le sottodirectory future.

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

4. Modifica in modo ricorsivo le autorizzazioni di file di `/var/www` e delle relative sottodirectory.

   ```
   [ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
   ```

> **Note**
>
> Se intendete utilizzarlo anche WordPress come server FTP, qui avrete bisogno di impostazioni di gruppo più permissive. Per eseguire questa operazione, consulta i passaggi e le impostazioni di sicurezza consigliati WordPress in.

5. Riavviare il server Web Apache per implementare il nuovo gruppo e le nuove autorizzazioni.
   - ```
     [ec2-user ~]$ sudo systemctl restart httpd
     ```

Esegui lo script WordPress di installazione con AL2

Sei pronto per l'installazione WordPress. I comandi utilizzati dipendono dal sistema operativo. I comandi di questa procedura possono essere utilizzati con AL2.

1. Utilizzare il comando systemctl per assicurarsi che i servizio `httpd` e di database vengano avviati a ogni avvio del sistema.

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

2. Verificare che il server di database sia in esecuzione.

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

   Se il servizio di database non è in esecuzione, avviarlo.

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

3. Verificare che il server Web Apache (`httpd`) sia in esecuzione.

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

   Se il servizio `httpd` non è in esecuzione, avviarlo.

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

4. In un browser Web, digita l'URL del tuo WordPress blog (l'indirizzo DNS pubblico dell'istanza o l'indirizzo seguito dalla `blog` cartella). Dovresti vedere lo script di WordPress installazione.
   ```

Fornisci le informazioni richieste dall' WordPress installazione. Per completare l'installazione, seleziona Installa WordPress. Per ulteriori informazioni, consulta Passaggio 5: Esecuzione dello script di installazione sul WordPress sito Web.

Fasi successive

Dopo aver testato il tuo WordPress blog, valuta la possibilità di aggiornarne la configurazione.

Utilizza un nome di dominio personalizzato

Se all'indirizzo EIP dell'istanza EC2 è associato un nome di dominio, puoi configurare il blog in modo che utilizzi tale nome anziché l'indirizzo DNS EC2 pubblico. Per ulteriori informazioni, consulta Modifica dell'URL del sito sul WordPress sito Web.

Configurazione del blog

Puoi configurare il blog in modo che utilizzi temi e plugin diversi in modo da offrire un'esperienza più personalizzata ai lettori. Tuttavia, il processo di installazione può talvolta generare problemi che portano alla perdita dell'intero blog. Pertanto, consigliamo vivamente di eseguire una copia di backup dell'Amazon Machine Image (AMI) dell'istanza prima di tentare di installare temi o plugin in modo da essere in grado di ripristinare il blog in caso di problemi durante l'installazione. Per ulteriori informazioni, consulta Creare la propria AMI.

Aumento della capacità

Se il tuo WordPress blog diventa popolare e hai bisogno di maggiore potenza di calcolo o spazio di archiviazione, prendi in considerazione i seguenti passaggi:

- Espandi lo spazio di storage sull'istanza. Per ulteriori informazioni, consulta Volumi elastici Amazon EBS nella Guida per l'utente di Amazon EBS.
- Trasferisci il database MySQL in Amazon RDS in modo da sfruttare tutte le funzionalità di scalabilità del servizio.

Miglioramento delle prestazioni di rete del traffico Internet

Se ti aspetti che il tuo blog gestisca il traffico da parte di utenti situati in tutto il mondo, considera l'uso di AWS Global Accelerator. Global Accelerator ti aiuta a ridurre la latenza migliorando le prestazioni del traffico Internet tra i dispositivi client degli utenti e l'applicazione su cui è in esecuzione

WordPress . AWS Global Accelerator utilizza la rete AWS globale per indirizzare il traffico verso un endpoint applicativo funzionante nella AWS regione più vicina al client.

Scopri di più su WordPress

Per informazioni in merito WordPress, consultate la documentazione di aiuto del WordPress Codex all'indirizzo http://codex.wordpress.org/.

Per ulteriori informazioni sulla risoluzione dei problemi di installazione, consulta Problemi di installazione comuni.

Per informazioni su come rendere il tuo WordPress blog più sicuro, consulta Hardening. WordPress

Per informazioni sulla gestione del WordPress blog up-to-date, consulta Aggiornamento WordPress.

Aiuto! Il nome DNS pubblico è cambiato e il blog non è accessibile

L' WordPress installazione viene configurata automaticamente utilizzando l'indirizzo DNS pubblico per l'istanza EC2. Se arresti e riavvii l'istanza, l'indirizzo DNS pubblico cambia, a meno che non sia associato a un indirizzo IP elastico, e il blog non funzionerà più perché fa riferimento a risorse disponibili in un indirizzo che non esiste più o che è assegnato a un'altra istanza EC2. Una descrizione più dettagliata del problema e diverse possibili soluzioni sono riportate in Modifica dell'URL del sito.

Se ciò si è verificato durante l' WordPress installazione, potrebbe essere possibile ripristinare il blog seguendo la procedura riportata di seguito, che utilizza l'interfaccia a riga di wp-cli comando per WordPress.

Per modificare l'URL del WordPress sito con wp-cli

1. Connettersi all'istanza EC2 con SSH.
2. Annotare il vecchio URL del sito e il nuovo URL del sito relativi all'istanza. Il vecchio URL del sito è probabilmente il nome DNS pubblico dell'istanza EC2 al momento dell'installazione. WordPress È possibile che il nuovo URL del sito sia il nome DNS pubblico corrente per l'istanza EC2. Se non sei certo del vecchio URL del sito, puoi utilizzare curl per cercarlo utilizzando il seguente comando.

   ```
   [ec2-user ~]$ curl localhost | grep wp-content
   ```

   I riferimenti al vecchio nome DNS pubblico dovrebbero essere presenti nell'output e sono simili a quanto segue (il vecchio URL del sito è visualizzato in rosso):

```
<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. Scaricare wp-cli con il seguente comando.

```
[ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/
phar/wp-cli.phar
```

4. Cerca e sostituisci il vecchio URL del sito nell' WordPress installazione con il seguente comando. Sostituisci il vecchio e il nuovo URL del sito con l'istanza EC2 e il percorso dell' WordPress installazione (di solito `/var/www/html` o). `/var/www/html/blog`

```
[ec2-user ~]$ php wp-cli.phar search-replace 'old_site_url' 'new_site_url' --path=/
path/to/wordpress/installation --skip-columns=guid
```

5. In un browser web, inserisci il nuovo URL del sito del tuo WordPress blog per verificare che il sito funzioni di nuovo correttamente. In caso contrario, consulta Modifica dell'URL del sito e Problemi di installazione comuni per ulteriori informazioni.

Utilizzo di Amazon Linux 2 al di fuori di Amazon EC2

Le immagini dei AL2 container possono essere eseguite in ambienti di runtime di container compatibili.

AL2 può anche essere eseguito come guest virtualizzato al di fuori dell'esecuzione diretta su Amazon EC2.

> **Note**
>
> La configurazione delle AL2 immagini è diversa da. AL2023
> Durante la migrazione a AL2023, assicurati di leggere la sezione Utilizzo di Amazon Linux 2023 al di fuori di Amazon EC2 e di adattare la configurazione per renderla compatibile con. AL2023

Esegui AL2 come macchina virtuale in locale

Usa le immagini della macchina AL2 virtuale (VM) per lo sviluppo e il test in locale. Offriamo un'immagine AL2 VM diversa per ciascuna delle piattaforme di virtualizzazione supportate. Puoi visualizzare l'elenco delle piattaforme supportate nella pagina Immagini di macchine virtuali Amazon Linux 2.

Per utilizzare le immagini delle macchine AL2 virtuali con una delle piattaforme di virtualizzazione supportate, procedi come segue:

- Fase 1: preparare l'immagine di avvio seed.iso
- Passaggio 2: scarica l'immagine della AL2 macchina virtuale
- Fase 3: avviare e connettere la nuova VM

Fase 1: preparare l'immagine di avvio `seed.iso`

L'immagine di avvio `seed.iso` include le informazioni di configurazione iniziale necessarie per avviare la tua nuova VM, quali la configurazione di rete, il nome host e i dati utente.

> **Note**
>
> L'immagine di avvio `seed.iso` include solo le informazioni di configurazione richieste per avviare la VM. Non include i file del sistema AL2 operativo.

Per generare l'immagine di avvio `seed.iso`, sono necessari due file di configurazione:

- `meta-data`: questo file include il nome host e le impostazioni di rete statiche per la VM.
- `user-data`: questo file configura gli account utente e ne specifica le password, le coppie di chiavi e i meccanismi d'accesso. Per impostazione predefinita, l'immagine della AL2 macchina virtuale crea un account `ec2-user` utente. Utilizza il `user-data` file di configurazione per impostare la password per l'account utente predefinito.

Per creare il **`seed.iso`** disco di avvio

1. Creare una nuova cartella denominata `seedconfig` e individuarla.
2. Crea il file di configurazione `meta-data`.
   a. Creare un nuovo file denominato `meta-data`.
   b. Aprire il file `meta-data` utilizzando l'editor preferito e aggiungere il seguente script.

```
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
```

   Sostituiscilo *`vm_hostname`* con un nome host VM a tua scelta e configura le impostazioni di rete come richiesto.
   c. Salva e chiudi il file di configurazione `meta-data`.

Per un esempio di file di configurazione `meta-data` che specifica un nome host VM (`amazonlinux.onprem`), configura l'interfaccia di rete predefinita (`eth0`) e specifica gli indirizzi IP statici per i dispositivi di rete necessari, vedi il file di esempio Seed.iso.

3. Crea il file di configurazione `user-data`.

   a. Creare un nuovo file denominato `user-data`.

   b. Aprire il file `user-data` utilizzando l'editor preferito e aggiungere il seguente script.

```
#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:'.
```

   Sostituiscilo *plain_text_password* con una password a tua scelta per l'account `ec2-user` utente predefinito.

   c. (Opzionale) Per impostazione predefinita, cloud-init applica le impostazioni di rete ad ogni avvio della VM. Aggiungere il seguente codice per impedire a cloud-init l'applicazione delle impostazioni di rete ad ogni avvio e per mantenere le impostazioni di rete applicate al primo avvio.

```
# 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. Salva e chiudi il file di configurazione `user-data`.

È anche possibile creare account utente aggiuntivi e specificarne i meccanismi d'accesso, le password e le coppie di chiavi. Per ulteriori informazioni sulle direttive supportate, consulta Riferimento ai moduli. Per un esempio di file `user-data` che crea utenti aggiuntivi e specifica una password personalizzata per l'account utente `ec2-user` predefinito, vedi il file di esempio Seed.iso.

4. Creare l'immagine di avvio `seed.iso` utilizzando `meta-data` e i file di configurazione `user-data`.

   Per Linux, utilizzare uno strumento come genisoimage. Navigare nella cartella `seedconfig` ed esegui il comando seguente.

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

   Per macOS, è possibile utilizzare uno strumento come hdiutil. Navigare a un livello superiore dalla cartella `seedconfig` ed esegui il comando seguente.

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

Passaggio 2: scarica l'immagine della AL2 macchina virtuale

Offriamo un'immagine AL2 VM diversa per ciascuna delle piattaforme di virtualizzazione supportate. Puoi visualizzare l'elenco delle piattaforme supportate e scaricare l'immagine VM corretta per la piattaforma scelta dalla pagina Immagini di macchine virtuali Amazon Linux 2.

Fase 3: avviare e connettere la nuova VM

Per avviare e connettersi alla nuova macchina virtuale, è necessario disporre dell'immagine di `seed.iso` avvio (creata nella fase 1) e di un'immagine della macchina AL2 virtuale (scaricata nella fase 2). I passaggi variano in base alla piattaforma VM scelta.

VMware vSphere

L'immagine VM per VMware è disponibile nel formato OVF.

Per avviare la macchina virtuale utilizzando vSphere VMware

1. Creare un nuovo datastore per il file `seed.iso` o aggiungerlo a un datastore esistente.
2. Distribuire il modello OVF, ma non avviare ancora la VM.
3. Nel pannello Navigator, fare clic con il pulsante destro del mouse sulla nuova macchina virtuale e scegliere Modifica impostazioni.
4. Nella scheda Hardware virtuale, per Nuovo dispositivo, scegliere Unità CD/DVD, quindi scegliere Aggiungi.
5. Per New CD/DVD Drive, scegli Datastore ISO File. Selezionare il datastore a cui è stato aggiunto il file `seed.iso`, individuare e selezionare il file `seed.iso`, quindi scegliere OK.
6. Per New CD/DVD Drive, seleziona Connect, quindi scegli OK.

Dopo aver associato il datastore alla VM, è possibile avviarlo.

KVM

Per avviare la VM mediante KVM

1. Aprire la Creazione guidata nuova VM .
2. Per Fase 1, scegliere Importa immagine disco esistente.
3. Per Fase 2, individuare e selezionare l'immagine VM. Per OS type (Tipo di sistema operativo) e Version (Versione), scegli rispettivamente Linux e Red Hat Enterprise Linux 7.0.
4. Per il passaggio 3, specifica la quantità di RAM e il numero di RAM CPUs da utilizzare.
5. Per Fase 4, immettere un nome per la nuova VM e selezionare Personalizza configurazione prima dell'installazione, quindi scegliere Fine.
6. Nella finestra Configurazione per la VM, scegliere Aggiungi hardware.
7. Nella finestra Add New Virtual Hardware (Aggiungi nuovo hardware virtuale), scegliere Storage (Archiviazione).
8. Nella Configurazione di archiviazione, scegliere Select or create custom storage (Seleziona o crea archiviazione personalizzata). Per Tipo di dispositivo, scegliere Dispositivo CDROM. Scegliere Gestisci, Sfoglia locale, quindi passare al file `seed.iso` e selezionarlo. Scegliere Finish (Fine).
9. Scegliere Inizia installazione.

Oracle VirtualBox

Per avviare la macchina virtuale utilizzando Oracle VirtualBox

1. Apri Oracle VirtualBox e scegli Nuovo.
2. In Name (Nome), inserisci un nome descrittivo per la macchina virtuale e per Type (Tipo) e Version (Versione) seleziona rispettivamente Linux e Red Hat (64-bit). Scegliere Continue (Continua).
3. Per Memory size (Dimensione memoria), specificare la quantità di memoria da allocare alla macchina virtuale, quindi scegliere Continue (Continua).
4. Per Hard disk (Disco rigido), scegliere Use an existing virtual hard disk file (Usa un file del disco rigido virtuale esistente), individuare e aprire l'immagine VM, quindi scegliere Create (Crea).
5. Prima di avviare la VM, è necessario caricare il file `seed.iso` nell'unità ottica virtuale della macchina virtuale:
   a. Selezionare la nuova VM, scegliere Settings (Impostazioni), quindi Storage (Archiviazione).
   b. Nell'elenco Storage Devices (Dispositivi di archiviazione), in Controller: IDE, scegliere l'unità ottica Empty (Vuota) .
   c. Nella sezione Attributi dell'unità ottica, scegliere il pulsante Sfoglia, selezionare Scegli file disco ottico virtuale, quindi selezionare il file `seed.iso`. Scegliere OK per applicare le modifiche e chiudere le impostazioni.

Dopo aver aggiunto il file `seed.iso` all'unità ottica virtuale, sarà possibile avviare la VM.

Microsoft Hyper-V

L'immagine VM per Microsoft Hyper-V viene compressa in un file zip. Estrai il contenuto del file .zip.

Per avviare la VM utilizzando Microsoft Hyper-V

1. Aprire la nuova procedura guidata macchina virtuale.
2. Quando viene richiesto di selezionare una generazione, scegliere Generazione 1.
3. Quando viene richiesto di configurare la scheda di rete, per Connessione scegliere Esterno.

4. Quando viene richiesto di connettersi a un disco rigido virtuale, scegliere Usa un disco rigido virtuale esistente, selezionare Sfoglia, quindi passare all'immagine della VM e selezionarla. Scegliere Termina per creare la VM.
5. Fare clic con il pulsante destro del mouse sulla nuova VM e scegliere Impostazioni. Nella finestra Impostazioni in Controller IDE 1, scegliere Unità DVD.
6. Per l'unità DVD, scegliere File immagine, quindi individuare il file `seed.iso` e selezionarlo.
7. Applicare le modifiche e avviare la VM.

Dopo l'avvio della VM, effettuare l'accesso utilizzando uno degli account utente definiti nel file di configurazione `user-data`. Dopo aver eseguito l'accesso per la prima volta, potrai disconnettere l'immagine di avvio `seed.iso`dalla VM.

Identificazione di istanze e versioni di Amazon Linux

Può essere importante essere in grado di determinare quale distribuzione Linux e quale versione di tale distribuzione è un'immagine o un'istanza del sistema operativo. Amazon Linux fornisce meccanismi per distinguere Amazon Linux dalle altre distribuzioni Linux, nonché per identificare a quale versione di Amazon Linux si riferisce l'immagine.

Questa sezione tratterà i diversi metodi che possono essere utilizzati, i relativi limiti e esaminerà alcuni esempi del loro utilizzo.

Argomenti

Utilizzo dello `os-release` standard

Amazon Linux è conforme allo `os-releasestandard` per l'identificazione delle distribuzioni Linux. Questo file fornisce informazioni leggibili da un computer sull'identificazione del sistema operativo e sulla versione.

> **Note**
>
> Lo standard impone che `/etc/os-release` si tenti di essere analizzato per primo, seguito da. `/usr/lib/os-release` È necessario prestare attenzione a seguire lo standard relativo ai nomi e ai percorsi dei file.

Argomenti

Principali differenze di identificazione

`os-release`Si trova in`/etc/os-release`, e se non è presente, in`/usr/lib/os-release`. Consulta lo `os-release`standard per informazioni complete.

Il modo più affidabile per determinare se un'istanza sta eseguendo Amazon Linux è quello di inserire il `ID` campo`os-release`.

Il modo più affidabile per distinguere tra le versioni consiste nel controllare il `VERSION_ID` campo in`os-release`:

- AMI Amazon Linux: `VERSION_ID` contiene una versione basata sulla data (ad es.) `2018.03`
- AL2: `VERSION_ID="2"`
- AL2023: `VERSION_ID="2023"`

> **Note**
>
> Ricorda che `VERSION_ID` è un campo leggibile da una macchina destinato all'uso programmatico, mentre `PRETTY_NAME` è progettato per essere visualizzato dagli utenti. the section called "Tipi di campo"Per ulteriori informazioni sui tipi di campo, vedere.

Tipi di campo: leggibile dalla macchina vs. leggibile dall'uomo

Il `/etc/os-release` file (o `/usr/lib/os-release` se `/etc/os-release` non esiste) contiene due tipi di campi: campi leggibili da computer destinati all'uso programmatico e campi leggibili dall'uomo destinati alla presentazione agli utenti.

Campi leggibili dalla macchina

Questi campi utilizzano formati standardizzati e sono destinati all'elaborazione mediante script, gestori di pacchetti e altri strumenti automatizzati. Contengono solo lettere minuscole, numeri e punteggiatura limitata (punti, trattini bassi e trattini).

- `ID`— Identificatore del sistema operativo. Amazon Linux lo utilizza `amzn` in tutte le versioni, distinguendolo da altre distribuzioni come Debian (`debian`), Ubuntu () o `ubuntu` Fedora () `fedora`

- `VERSION_ID`— Versione del sistema operativo per uso programmatico (ad es.) `2023`
- `ID_LIKE`— Elenco separato da spazi delle distribuzioni correlate (ad es.) `fedora`
- `VERSION_CODENAME`— Nome in codice di rilascio per gli script (ad es.) `karoo`
- `VARIANT_ID`— Identificatore di variante per le decisioni programmatiche
- `BUILD_ID`— Crea un identificatore per le immagini di sistema
- `IMAGE_ID`— Identificatore di immagine per ambienti containerizzati
- `PLATFORM_ID`— Identificatore della piattaforma (ad es.) `platform:al2023`

Campi leggibili dall'uomo

Questi campi sono destinati alla visualizzazione da parte degli utenti e possono contenere spazi, lettere maiuscole e minuscole e testo descrittivo. Dovrebbero essere usati quando si presentano informazioni sul sistema operativo nelle interfacce utente.

- `NAME`— Nome del sistema operativo da visualizzare (ad esempio,`Amazon Linux`)
- `PRETTY_NAME`— Nome completo del sistema operativo con versione da visualizzare (ad es.`Amazon Linux 2023.8.20250721`)
- `VERSION`— Informazioni sulla versione adatte alla presentazione all'utente
- `VARIANT`— Nome della variante o dell'edizione da visualizzare (ad es.`Server Edition`)

Altri campi informativi

Questi campi forniscono metadati aggiuntivi sul sistema operativo:

- `HOME_URL`— URL della home page del progetto
- `DOCUMENTATION_URL`— URL della documentazione
- `SUPPORT_URL`— URL delle informazioni di supporto
- `BUG_REPORT_URL`— URL di segnalazione dei bug
- `VENDOR_NAME`— Nome del fornitore
- `VENDOR_URL`— URL del fornitore
- `SUPPORT_END`— End-of-support data in formato YYYY-MM-DD
- `CPE_NAME`— Identificatore comune di enumerazione della piattaforma
- `ANSI_COLOR`— Codice a colori ANSI per la visualizzazione del terminale

Quando scrivi script o applicazioni che devono identificare Amazon Linux a livello di codice, usa campi leggibili dalla macchina come e. `ID` `VERSION_ID` Quando mostri informazioni sul sistema operativo agli utenti, usa campi leggibili dall'uomo come. `PRETTY_NAME`

Esempi di **`/etc/os-release`**

Il contenuto dei `/etc/os-release` file varia tra le versioni di Amazon Linux:

AL2023

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

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

AL2

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

```
NAME="Amazon Linux"
VERSION="2"
ID="amzn"
ID_LIKE="centos rhel fedora"
VERSION_ID="2"
PRETTY_NAME="Amazon Linux 2"
ANSI_COLOR="0;33"
```

```
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2"
HOME_URL="https://amazonlinux.com/"
SUPPORT_END="2026-06-30"
```

Amazon Linux AMI

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

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

Confronto con altre distribuzioni

Per capire come Amazon Linux si inserisce nel più ampio ecosistema Linux, confronta il suo `/etc/os-release` formato con le altre principali distribuzioni:

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
```

Nota come i campi leggibili dalla macchina forniscono un'identificazione coerente tra le distribuzioni:

- `ID`— Identifica in modo univoco il sistema operativo: per `amzn` Amazon Linux, `fedora` per Fedora, per Debian, `debian` per Ubuntu `ubuntu`
- `ID_LIKE`— Mostra le relazioni di distribuzione: Amazon Linux usa `fedora` (AL2023) o `centos rhel fedora` (AL2), mentre Ubuntu mostra `debian` per indicare la sua eredità Debian
- `VERSION_ID`— Fornisce informazioni sulla versione analizzabili automaticamente: `2023` per AL2 023, per Fedora, per Debian, `42` per Ubuntu `12` `24.04`

Al contrario, i campi leggibili dall'uomo sono progettati per essere visualizzati agli utenti:

- `NAME`— Nome del sistema operativo intuitivo:,,, `Amazon Linux` `Fedora Linux` `Debian GNU/Linux` `Ubuntu`
- `PRETTY_NAME`— Nome visualizzato completo con versione:`Amazon Linux 2023.8.20250721`,,`Fedora Linux 42 (Container Image)`, `Debian GNU/Linux 12 (bookworm)` `Ubuntu 24.04.2 LTS`
- `VERSION`— Versione leggibile dall'uomo con contesto aggiuntivo come nomi in codice o tipi di versione

Quando scrivi script multipiattaforma, usa sempre i campi leggibili dalla macchina (, `IDVERSION_ID`,`ID_LIKE`) per la logica e le decisioni e usa i campi leggibili dall'uomo (,) solo per mostrare informazioni agli utenti. `PRETTY_NAME` `NAME`

Specifico per Amazon Linux

Esistono alcuni file specifici di Amazon Linux che possono essere utilizzati per identificare Amazon Linux e la sua versione. Il nuovo codice deve utilizzare lo `/etc/os-release` standard per essere compatibile con più distribuzioni. L'uso di file specifici di Amazon Linux è sconsigliato.

Argomenti

- Il file /etc/system-release
- File di identificazione dell'immagine
- Esempi di file specifici per Amazon Linux

Il file `/etc/system-release`

Amazon Linux include un file `/etc/system-release` che specifica la versione corrente installata. Questo file viene aggiornato utilizzando i gestori di pacchetti e su Amazon Linux fa parte del `system-release` pacchetto. Anche se alcune altre distribuzioni come Fedora hanno questo file, esso non è presente nelle distribuzioni basate su Debian come Ubuntu.

> **Note**
>
> Il `/etc/system-release` file contiene una stringa leggibile dall'uomo e non deve essere usato a livello di codice per identificare un sistema operativo o una versione. Utilizza invece i campi leggibili dalla macchina in `/etc/os-release` (o se non esiste). `/usr/lib/os-release` `/etc/os-release`

Amazon Linux contiene anche una versione leggibile dalla macchina `/etc/system-release` che segue la specifica Common Platform Enumeration (CPE) nel file. `/etc/system-release-cpe`

File di identificazione dell'immagine

Ogni immagine Amazon Linux contiene un `/etc/image-id` file univoco che fornisce informazioni aggiuntive sull'immagine originale generata dal team di Amazon Linux. Questo file è specifico di Amazon Linux e non si trova in altre distribuzioni Linux come Debian, Ubuntu o Fedora. Questo file contiene le seguenti informazioni relative all'immagine:

- `image_name`,`image_version`, `image_arch` — Valori della ricetta di compilazione utilizzata per costruire l'immagine.
- `image_stamp`: un valore esadecimale casuale univoco generato durante la creazione dell'immagine.
- `image_date`— L'ora UTC di creazione dell'immagine, in YYYYMMDDhhmmssformato.
- `recipe_name`, `recipe_id` — Il nome e l'ID della ricetta di compilazione utilizzata per costruire l'immagine.

Esempi di file specifici per Amazon Linux

Le seguenti sezioni forniscono esempi di file di identificazione specifici di Amazon Linux per ogni versione principale di Amazon Linux.

> **Note**
>
> In qualsiasi codice reale, `/usr/lib/os-release` dovrebbe essere usato se il `/etc/os-release` file non esiste.

AL2023

Gli esempi seguenti mostrano i file di identificazione per AL2 023.

Esempio di `/etc/image-id` AL2 023:

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

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

Esempio di `/etc/system-release` AL2 023:

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

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

AL2

Gli esempi seguenti mostrano i file di identificazione per AL2.

Esempio di `/etc/image-id` per 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"
```

Esempio di `/etc/system-release` per AL2:

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

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

Amazon Linux AMI

Gli esempi seguenti mostrano i file di identificazione per l'AMI Amazon Linux.

Esempio `/etc/image-id` di AMI Amazon Linux:

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

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

Esempio `/etc/system-release` di AMI Amazon Linux:

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

```
Amazon Linux AMI release 2018.03
```

Codice di esempio per il rilevamento del sistema operativo

Gli esempi seguenti mostrano come rilevare a livello di codice il sistema operativo e la versione utilizzando il file `/etc/os-release` (o `/usr/lib/os-release` se `/etc/os-release` non

esiste). Questi esempi mostrano come distinguere tra Amazon Linux e altre distribuzioni, nonché come utilizzare il `ID_LIKE` campo per determinare le famiglie di distribuzione.

Lo script seguente è implementato in diversi linguaggi di programmazione e ogni implementazione produrrà lo stesso risultato.

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";
    }
}
```

Quando viene eseguito su sistemi diversi, lo script produrrà il seguente output:

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)
```

AWSintegrazione in AL2

AWSstrumenti da riga di comando

AWS Command Line Interface(AWS CLI) è uno strumento open source che fornisce un'interfaccia coerente con cui interagire Servizi AWS utilizzando i comandi nella shell della riga di comando. Per ulteriori informazioni, consulta What is the? AWS Command Line Interface nella Guida AWS Command Line Interface per l'utente.

AL2 e AL1 hanno la versione 1 AWS CLI preinstallata. L'attuale versione di Amazon Linux, AL2 023, ha la versione 2 AWS CLI preinstallata. Per ulteriori informazioni sull'utilizzo di AWS CLI on AL2 023, consulta Get started with AL2 023 nella Amazon Linux 2023 User Guide.

Nozioni di base sui runtime di programmazione

AL2 fornisce versioni diverse di runtime di determinati linguaggi. Lavoriamo con progetti upstream, come PHP, che supportano più versioni contemporaneamente. Per trovare informazioni su come installare e gestire questi pacchetti con versione del nome, usa il `yum` comando per cercare e installare questi pacchetti. Per ulteriori informazioni, consulta Archivio dei pacchetti.

Gli argomenti seguenti descrivono il funzionamento di ogni linguaggio di runtime in. AL2

Argomenti

- CC++, e Fortran in AL2
- Entra AL2
- Javanel AL2
- Perlnel AL2
- PHPnel AL2
- Pythonnel AL2
- Arruggine AL2

CC++, e Fortran in AL2

AL2 include sia la GNU Compiler Collection (GCC) che il Clang frontend per. LLVM

La versione principale di GCC rimarrà costante per tutta la durata di. AL2 Le correzioni di bug e sicurezza potrebbero essere trasferite nella versione principale di GCC cui è disponibile. AL2

Per impostazione predefinita, AL2 include la versione 7.3 di GCC cui compila quasi tutti i pacchetti. Il `gcc10` pacchetto ne rende disponibili GCC 10 in misura limitata, ma non è consigliabile utilizzarne GCC 10 per creare pacchetti.

I flag predefiniti del compilatore che compila AL2 RPMs includono alcuni flag di ottimizzazione e rafforzamento. Ti consigliamo di includere alcuni flag di ottimizzazione e rafforzamento se stai creando il tuo codice con. GCC

Il compilatore e i flag di ottimizzazione predefiniti in AL2 023 migliorano ciò che è presente in. AL2

Entra AL2

Potresti voler creare il tuo codice scritto Gosu Amazon Linux utilizzando una toolchain fornita con AL2.

La Go toolchain verrà aggiornata per tutta la durata di. AL2 Ciò potrebbe avvenire in risposta a qualsiasi CVE presente nella toolchain che spediamo o come prerequisito per indirizzare un CVE in un altro pacchetto.

Goè un linguaggio di programmazione che si muove relativamente velocemente. Potrebbe esserci una situazione in cui le applicazioni esistenti scritte Go devono adattarsi alle nuove versioni della Go toolchain. Per ulteriori informazioni suGo, vedere Go1 and the Future of Go Programs.

Sebbene AL2 incorporerà nuove versioni della Go toolchain nel corso del suo ciclo di vita, ciò non sarà in linea con le versioni precedenti. Go Pertanto, l'utilizzo della Go toolchain fornita AL2 potrebbe non essere adatto se si desidera creare Go codice utilizzando funzionalità all'avanguardia del linguaggio e della libreria standard. Go

Durante la vita di AL2, le versioni precedenti dei pacchetti non vengono rimosse dai repository. Se è necessaria una Go toolchain precedente, potete scegliere di rinunciare alle correzioni di bug e di sicurezza delle Go toolchain più recenti e installare una versione precedente dai repository utilizzando gli stessi meccanismi disponibili per qualsiasi RPM.

Se desideri creare il tuo Go codice su di esso, AL2 puoi utilizzare la Go toolchain inclusa AL2 con la consapevolezza che questa toolchain potrebbe andare avanti per tutta la vita di. AL2

Javanel AL2

AL2 fornisce diverse versioni di Amazon Corretto per supportare carichi di lavoro Java basati, oltre ad alcune OpenJDK versioni. Ti consigliamo di effettuare la migrazione ad Amazon Corretto prima di passare alla AL2 versione 023.

Corretto è una build dell'Open Java Development Kit (OpenJDK) con supporto a lungo termine da. Amazon Corretto è certificato utilizzando il Java Technical Compatibility Kit (TCK) per garantire che soddisfi lo standard Java SE e sia disponibile su LinuxWindows, emacOS.

Un pacchetto Amazon Corretto è disponibile per ciascuno dei pacchetti Corretto 1.8.0, Corretto 11 e Corretto 17.

Ogni versione di Corretto in AL2 è supportata per lo stesso periodo di tempo della versione Corretto, o fino alla fine del ciclo di vita di, a seconda di quale delle due AL2 situazioni si verifichi per prima. Per ulteriori informazioni, consulta Amazon Corretto FAQs.

Perlnel AL2

AL2 fornisce la versione 5.16 del linguaggio di Perlprogrammazione.

Perlmoduli in AL2

Vari Perl moduli sono confezionati come RPMs in AL2. Sebbene siano disponibili molti Perl moduli RPMs, Amazon Linux non cerca di impacchettare tutti i Perl moduli possibili. Moduli confezionati come RPMs potrebbero essere utilizzati da altri pacchetti RPM del sistema operativo, quindi Amazon Linux darà la priorità alla garanzia che siano dotati di patch di sicurezza rispetto ai puri aggiornamenti delle funzionalità.

AL2 consente inoltre `CPAN` Perl agli sviluppatori di utilizzare il gestore di pacchetti idiomatico per i moduli. Perl

PHPnel AL2

AL2 attualmente fornisce due versioni completamente supportate del linguaggio di PHPprogrammazione come parte diAL2 Libreria Extras. Ogni PHP versione è supportata per lo stesso periodo di tempo della versione upstream PHP elencata nella sezione deprecated date in. Elenco degli extra di Amazon Linux 2

Per informazioni su come utilizzare AL2 Extras per installare aggiornamenti di applicazioni e software sulle istanze, consulta. AL2 Libreria Extras

Per facilitare la migrazione a AL2 023, sono disponibili sia PHP 8.1 che 8.2 su e 023. AL2 AL2

> **Note**
>
> AL2 include PHP 7,1, 7,2, 7,3 e 7,4 pollici. `amazon-linux-extras` Tutti questi extra sono EOL e non è garantito che ricevano aggiornamenti di sicurezza aggiuntivi.
> Per scoprire quando ogni versione di PHP è obsoleta, consulta il. AL2 Elenco degli extra di Amazon Linux 2

Migrazione da versioni 8.x precedenti PHP

La PHP comunità upstream ha redatto una documentazione completa sulla migrazione per passare alla versione PHP 8.2 dalla 8.1. PHP Esiste anche la documentazione per la migrazione dalla versione PHP 8.0 alla 8.1.

AL2 include PHP 8.0, 8.1 e 8.2 e consente un percorso di aggiornamento efficiente a `amazon-linux-extras` 023. AL2 Per scoprire quando ogni versione di PHP è obsoleta in, consulta. AL2 Elenco degli extra di Amazon Linux 2

Migrazione da PHP versioni 7.x

La PHP comunità upstream ha messo insieme una documentazione completa sulla migrazione per passare alla PHP versione 8.0 dalla 7.4. PHP Oltre alla documentazione citata nella sezione precedente sulla migrazione alla versione PHP 8.1 e PHP 8.2, sono disponibili tutti i passaggi necessari per migrare l'applicazione basata su una versione moderna. PHP PHP

Il PHPprogetto mantiene un elenco e una pianificazione delle versioni supportate, insieme a un elenco di rami non supportati.

> **Note**
>
> Quando AL2 023 è stato rilasciato, tutte le versioni 7.x e 5.x di 023 non PHPerano supportate dalla PHPcommunity e non erano incluse come opzioni in 023. AL2

Pythonnel AL2

AL2 fornisce supporto e patch di sicurezza per la versione Python 2.7 fino a giugno 2026, come parte del nostro impegno di supporto a lungo termine per i pacchetti AL2 principali. Questo supporto va oltre la dichiarazione della Python community upstream del Python 2.7 EOL di gennaio 2020.

> **Note**
>
> AL2023 ha completamente rimosso 2.7. Python Tutti i componenti che lo richiedono Python sono ora scritti per funzionare con Python 3.

AL2 utilizza il gestore di `yum` pacchetti che ha una forte dipendenza da Python 2.7. Nella versione AL2 023, il gestore di `dnf` pacchetti è migrato alla versione Python 3 e non richiede più la versione 2.7. Python AL2023 è stato completamente spostato su 3. Python Ti consigliamo di completare la migrazione a Python 3.

Arruggine AL2

Potresti voler creare il tuo codice scritto AL2 utilizzando una toolchain fornita con AL2. Rust

La Rust toolchain verrà aggiornata per tutta la durata di. AL2 Ciò potrebbe avvenire in risposta a un CVE nella toolchain che forniamo o come prerequisito per un aggiornamento CVE in un altro pacchetto.

Rustè un linguaggio che si muove relativamente velocemente, con nuove versioni a una cadenza di circa sei settimane. Le nuove versioni potrebbero aggiungere nuove funzionalità linguistiche o di libreria standard. Sebbene AL2 incorporerà nuove versioni della Rust toolchain nel corso del suo ciclo di vita, ciò non sarà in linea con le versioni precedenti. Rust Pertanto, l'utilizzo della Rust toolchain fornita AL2 potrebbe non essere adatto se si desidera creare Rust codice utilizzando funzionalità all'avanguardia del linguaggio. Rust

Durante la durata di AL2, le versioni precedenti dei pacchetti non vengono rimosse dai repository. Se è necessaria una Rust toolchain precedente, potete scegliere di rinunciare alle correzioni di bug e di sicurezza delle Rust toolchain più recenti e di installare una versione precedente dai repository utilizzando gli stessi processi disponibili per qualsiasi RPM.

Su cui creare il tuo Rust codice AL2, usa la Rust toolchain inclusa nella confezione sapendo che questa toolchain AL2 potrebbe funzionare per tutta la vita di. AL2

AL2 kernel

AL2 originariamente fornito con un kernel 4.14, con la versione 5.10 come impostazione predefinita corrente. Se si utilizza ancora un kernel 4.14, si consiglia di migrare al kernel 5.10.

Il kernel live patching è supportato su. AL2

Argomenti

AL2 kernel supportati

Versioni di kernel supportate

Attualmente AL2 AMIs sono disponibili con le versioni del kernel 4.14 e 5.10, con la versione 5.10 come predefinita. Ti consigliamo di utilizzare un' AL2 AMI con kernel 5.10.

AL2023 AMIs sono disponibili con la versione del kernel 6.1. Per ulteriori informazioni, consulta la sezione Modifiche del AL2023 kernel AL2 nella Guida per l'utente di Amazon Linux 2023.

Tempistiche del supporto

Il kernel 5.10 disponibile su AL2 sarà supportato fino alla fine del supporto standard per l' AL2 AMI.

Supporto dell'applicazione di patch live

AL2 versione del kernel	Supporto delle patch live del kernel
4.14	Sì
5,10	Sì
5,15	No

Kernel Live Patching attivo AL2

> **Important**
>
> Amazon Linux interromperà l'applicazione di patch live per AL2 Kernel 4.14 il 31/10/2025. I clienti sono incoraggiati a utilizzare il kernel 5.10 come kernel predefinito per AL2 (vedi kernel AL2 supportati) o a passare ai kernel 6.1 e 6.12. AL2023
> Amazon Linux fornirà patch live per AL2 Kernel 5.10 fino alla fine del ciclo di AL2 vita, il 30/06/2020.

Kernel Live Patching for AL2 consente di applicare vulnerabilità di sicurezza specifiche e patch di bug critici a un kernel Linux in esecuzione, senza riavvii o interruzioni delle applicazioni in esecuzione. Ciò consente di beneficiare di una migliore disponibilità dei servizi e delle applicazioni, applicando queste correzioni fino al riavvio del sistema.

Per informazioni su Kernel Live Patching for AL2023, consulta Kernel Live Patching on nella Amazon Linux 2023 AL2023 User Guide.

AWS rilascia due tipi di patch live del kernel per: AL2

- Aggiornamenti di sicurezza: includono aggiornamenti per CVE (Common Vulnerabilities and Exposures) di Linux. Questi aggiornamenti sono in genere classificati come importanti o critici utilizzando le classificazioni di Amazon Linux Security Advisory. Generalmente vengono mappati a un punteggio CVSS (Common Vulnerability Scoring System) di 7 o superiore. In alcuni casi, AWS potrebbe fornire aggiornamenti prima dell'assegnazione di un CVE. In questi casi, le patch potrebbero apparire come correzioni di bug.
- Correzioni di bug: includono correzioni di bug critici e problemi di stabilità non associati a. CVEs

AWS fornisce patch live del kernel per una versione del AL2 kernel per un massimo di 3 mesi dopo il suo rilascio. Dopo il periodo di 3 mesi, è necessario eseguire l'aggiornamento a una versione del kernel successiva per continuare a ricevere patch live del kernel.

AL2 le patch live del kernel sono rese disponibili come pacchetti RPM firmati nei repository esistenti. AL2 Le patch possono essere installate su singole istanze utilizzando i flussi di lavoro yum esistenti oppure possono essere installate su un gruppo di istanze gestite utilizzando Systems Manager. AWS

Kernel Live Patching on AL2 viene fornito senza costi aggiuntivi.

Argomenti

Configurazioni e prerequisiti supportati

Kernel Live Patching è supportato sulle istanze Amazon EC2 e sulle macchine virtuali locali in esecuzione. AL2

Per utilizzare Kernel Live Patching su, devi usare: AL2

- Versione del kernel `4.14` o `5.10` sull'architettura `x86_64`
- Versione del kernel `5.10` sull'architettura `ARM64`

Requisiti per le policy

Per scaricare pacchetti dai repository Amazon Linux, Amazon EC2 deve accedere ai bucket Amazon S3 di proprietà del servizio. Se utilizzi un endpoint del cloud privato virtuale (VPC) di Amazon per Amazon S3 nel tuo ambiente, devi assicurarti che la policy degli endpoint VPC consenta l'accesso a tali bucket pubblici.

La tabella descrive ciascuno dei bucket Amazon S3 di cui EC2 potrebbe aver bisogno per accedere a Kernel Live Patching.

ARN di bucket S3	Description
arn:aws:s3: :pacchetti. *region*.amazonaws.com/*	Bucket Amazon S3 contenente i pacchetti AMI Amazon Linux
arn:aws:s3: ::repo. *region*.amazonaws.com/*	Bucket Amazon S3 contenente i repository AMI Amazon Linux
arn:aws:s3: ::amazonlinux. *region*.amazonaws.com/*	Bucket Amazon S3 contenente repository AL2

ARN di bucket S3	Description
arn:aws:s3: :amazonlinux-2-repos- /* *region*	Bucket Amazon S3 contenente repository AL2

La policy seguente illustra come limitare l'accesso alle identità e alle risorse che appartengono alla tua organizzazione e fornire l'accesso ai bucket Amazon S3 richiesti per Kernel Live Patching. Sostituisci *region* *principal-org-id* e *resource-org-id* con i valori della tua organizzazione.

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/*"
      ]
    }
  ]
}
```

Utilizzo di Kernel Live Patching

È possibile abilitare e utilizzare Kernel Live Patching su singole istanze utilizzando la riga di comando sull'istanza stessa oppure è possibile abilitare e utilizzare Kernel Live Patching su un gruppo di istanze gestite utilizzando Systems Manager. AWS

Le sezioni seguenti spiegano come abilitare e utilizzare Kernel Live Patching su singole istanze utilizzando la riga di comando.

Per ulteriori informazioni sull'attivazione e l'utilizzo di Kernel Live Patching su un gruppo di istanze gestite, consulta Use Kernel Live Patching sulle istanze nella Guida per l'utente. AL2 AWS Systems Manager

Argomenti

Abilitazione di Kernel Live Patching

Kernel Live Patching è disabilitato per impostazione predefinita su. AL2 Per utilizzare l'applicazione di patch live, è necessario installare il plugin yum per Kernel Live Patching e abilitare la funzionalità di applicazione di patch live.

Prerequisiti

L'applicazione di patch live del kernel richiede `binutils`. Se `binutils` non è stato installato, installarlo utilizzando il seguente comando:

```
$ sudo yum install binutils
```

Per abilitare Kernel Live Patching

1. Le patch live del kernel sono disponibili per le seguenti versioni del kernel: AL2

   - Versione del kernel `4.14` o `5.10` sull'architettura `x86_64`
   - Versione del kernel `5.10` sull'architettura `ARM64`

   Per controllare la versione del kernel, eseguire il seguente comando.

   ```
   $ sudo yum list kernel
   ```

2. Se si dispone già di una versione del kernel supportata, ignorare questa fase. Se non si dispone di una versione del kernel supportata, eseguire i seguenti comandi per aggiornare il kernel alla versione più recente e riavviare l'istanza.

   ```
   $ sudo yum install -y kernel
   ```

   ```
   $ sudo reboot
   ```

3. Installare il plugin yum per Kernel Live Patching.

   ```
   $ sudo yum install -y yum-plugin-kernel-livepatch
   ```

4. Abilitare il plugin yum per Kernel Live Patching.

   ```
   $ sudo yum kernel-livepatch enable -y
   ```

   Questo comando installa anche l'ultima versione dell'RPM della patch live del kernel dai repository configurati.

5. Per confermare che il plugin yum per Kernel Live Patching è stato installato correttamente, eseguire il seguente comando.

   ```
   $ rpm -qa | grep kernel-livepatch
   ```

Quando si abilita Kernel Live Patching, viene automaticamente applicata una RPM della patch live del kernel vuota. Se Kernel Live Patching è stata abilitata correttamente, questo comando restituisce un elenco che include l'RPM della patch live del kernel vuota iniziale. Di seguito è riportato un output di esempio.

```
yum-plugin-kernel-livepatch-1.0-0.11.amzn2.noarch
kernel-livepatch-5.10.102-99.473-1.0-0.amzn2.x86_64
```

6. Installare il pacchetto kpatch.

```
$ sudo yum install -y kpatch-runtime
```

7. Aggiornare il servizio kpatch se è stato precedentemente installato.

```
$ sudo yum update kpatch-runtime
```

8. Avviare il servizio kpatch. Questo servizio carica tutte le patch live del kernel dopo l'inizializzazione o l'avvio.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

9. Abilita l'argomento Kernel Live Patching nella libreria Extras. AL2 Questo argomento contiene le patch live del kernel.

```
$ sudo amazon-linux-extras enable livepatch
```

Visualizzazione delle patch live del kernel disponibili

Gli avvisi di sicurezza di Amazon Linux vengono pubblicati nel Centro di Sicurezza Amazon Linux. Per ulteriori informazioni sugli avvisi AL2 di sicurezza, che includono avvisi per le patch live del kernel, consulta Amazon Linux Security Center. Le patch live del kernel sono precedute da `ALASLIVEPATCH`. Centro di Sicurezza Amazon Linux potrebbe non elencare le patch live del kernel che risolvono i bug.

Puoi anche scoprire le patch live del kernel disponibili per ricevere avvisi e utilizzare la riga di comando. CVEs

Per elencare tutte le patch live del kernel disponibili per le consulenze

Utilizzare il seguente comando.

```
$ yum updateinfo list
```

Di seguito viene mostrato l'output di esempio.

```
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
```

Per elencare tutte le patch live del kernel disponibili per CVEs

Utilizza il seguente comando.

```
$ yum updateinfo list cves
```

Di seguito viene mostrato l'output di esempio.

```
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
```

Applicazione delle patch live del kernel

Le patch live del kernel vengono applicate utilizzando il gestore di pacchetti yum nello stesso modo in cui si applicano aggiornamenti regolari. Il plugin yum per Kernel Live Patching gestisce le patch live del kernel disponibili per essere applicate.

> **Tip**
>
> Si consiglia di aggiornare regolarmente il kernel utilizzando Kernel Live Patching per garantire che riceva correzioni di sicurezza specifiche, importanti e critiche fino al riavvio del sistema. Controlla anche se sono state rese disponibili correzioni aggiuntive al pacchetto kernel nativo

che non possono essere distribuite come patch live e aggiorna e riavvia con l'aggiornamento del kernel in questi casi.

Puoi scegliere di applicare una patch live del kernel specifica o applicare qualsiasi patch live del kernel disponibile insieme ai normali aggiornamenti di sicurezza.

Per applicare una patch live del kernel specifica

1. Ottenere la versione della patch live del kernel utilizzando uno dei comandi descritti in Visualizzazione delle patch live del kernel disponibili.
2. Applica la kernel live patch per il tuo kernel. AL2

```
$ sudo yum install kernel-livepatch-kernel_version.x86_64
```

Ad esempio, il seguente comando applica una patch live del kernel per la versione kernel AL2 `5.10.102-99.473`.

```
$ sudo yum install kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
```

Per applicare eventuali patch live del kernel disponibili insieme ai normali aggiornamenti di sicurezza

Utilizzare il seguente comando.

```
$ sudo yum update --security
```

Omettere l'opzione `--security` per includere correzioni di bug.

Important

- La versione del kernel non viene aggiornata dopo l'applicazione delle patch live del kernel. La versione viene aggiornata alla nuova versione solo dopo il riavvio dell'istanza.
- Un AL2 kernel riceve le patch live del kernel per un periodo di tre mesi. Dopo che è scaduto, non vengono rilasciate nuove patch live del kernel per tale versione del kernel. Per continuare a ricevere patch live del kernel dopo il periodo di tre mesi, è necessario riavviare l'istanza per passare alla nuova versione del kernel, che quindi continuerà a

ricevere le patch live del kernel per i tre mesi successivi. Per controllare la finestra di supporto per la versione del kernel, eseguire `yum kernel-livepatch supported`.

Visualizzazione delle patch live del kernel applicate

Per visualizzare le patch live del kernel applicate

Utilizzare il seguente comando.

```
$ kpatch list
```

Il comando restituisce un elenco delle patch live del kernel dell'aggiornamento di sicurezza caricato e installato. Di seguito è riportato un output di esempio.

```
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**
>
> Una singola patch live del kernel può includere e installare più patch live.

Disabilitazione di Kernel Live Patching

Se non è più necessario utilizzare Kernel Live Patching, puoi disabilitarla in qualsiasi momento.

Per disabilitare Kernel Live Patching

1. Rimuovere i pacchetti RPM per le patch live del kernel applicate.

   ```
   $ sudo yum kernel-livepatch disable
   ```

2. Disinstallare il plugin yum per Kernel Live Patching.

```
$ sudo yum remove yum-plugin-kernel-livepatch
```

3. Riavviare l'istanza.

```
$ sudo reboot
```

Limitazioni

Kernel Live Patching presenta le seguenti restrizioni:

- Durante l'applicazione di una patch live del kernel, non puoi eseguire l'ibernazione, usare strumenti di debug avanzati (come SystemTap kprobes e strumenti basati su EBPF) o accedere ai file di output ftrace usati dall'infrastruttura Kernel Live Patching.
-

> **Note**
>
> A causa di limitazioni tecniche, alcuni problemi non possono essere risolti con live patching. Per questo motivo, queste correzioni non verranno incluse nel pacchetto kernel live patch ma solo nell'aggiornamento del pacchetto kernel nativo. È possibile installare l'aggiornamento del pacchetto del kernel nativo e riavviare il sistema per attivare le patch come al solito.

Domande frequenti

Per domande frequenti su Kernel Live Patching for AL2, consulta le domande frequenti su Amazon Linux 2 Kernel Live Patching.

AL2 Libreria Extras

> **Warning**
>
> L'`epel`Extra abilita l'archivio di terze parti. EPEL7 A partire dal 30/06/2020, l'EPEL7archivio di terze parti non viene più mantenuto.
> Questo repository di terze parti non avrà aggiornamenti futuri. Ciò significa che non ci saranno correzioni di sicurezza per i pacchetti nell'archivio EPEL.
> Consulta la EPELsezione della Guida per l'utente di Amazon Linux 2023 per le opzioni di alcuni EPEL pacchetti.

Con AL2, puoi utilizzare la libreria Extras per installare aggiornamenti di applicazioni e software sulle tue istanze. Questi aggiornamenti di software sono definiti argomenti. Puoi installare una versione specifica di un argomento oppure omettere le informazioni sulla versione per utilizzare la versione più recente. Gli extra aiutano a ridurre il rischio di dover scendere a compromessi tra la stabilità di un sistema operativo e la freschezza del software disponibile.

I contenuti degli argomenti Extras sono esenti dalla politica di Amazon Linux sul supporto a lungo termine e sulla compatibilità binaria. Gli argomenti Extras forniscono l'accesso a un elenco curato di pacchetti. Le versioni dei pacchetti potrebbero essere aggiornate frequentemente o potrebbero non essere supportate per lo stesso periodo di tempo di. AL2

> **Note**
>
> I singoli argomenti di Extras potrebbero essere obsoleti prima che raggiungano l'EOL. AL2

Per elencare gli argomenti disponibili, utilizzare il comando seguente.

```
[ec2-user ~]$ amazon-linux-extras list
```

Per abilitare un argomento e installare la versione più recente del relativo pacchetto per assicurarne la freschezza, utilizzate il comando seguente.

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

Per abilitare gli argomenti e installare versioni specifiche dei relativi pacchetti per garantire la stabilità, utilizzate il comando seguente.

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

Per rimuovere un pacchetto installato da un argomento, utilizzare il comando seguente.

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk
 '{ print $1 }')
```

> **Note**
>
> Questo comando non rimuove i pacchetti che sono stati installati come dipendenze di Extra.

Per disabilitare un argomento e rendere i pacchetti inaccessibili al gestore di pacchetti yum, usa il seguente comando.

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

> **Important**
>
> Questo comando è destinato agli utenti avanzati. L'utilizzo improprio di questo comando può causare conflitti di compatibilità dei pacchetti.

Elenco degli extra di Amazon Linux 2

Nome aggiuntivo	Data obsoleta
BCC	
GraphicsMagick1.3	
R3.4	
R4	

Nome aggiuntivo	Data obsoleta
ansibile 2	2023-09-30
aws-nitro-enclaves-cli	
awscli1	
collectd	
collezione-python3	
corretto8	
dnsmasq	
dnsmasq2.85	2025-05-01
docker	
ecs	
emacs	2018-11-14
respingere	2024-06-30
petardo	2022-11-08
firefox	
gimp	2018-11-14
golang 1.11	2023-08-01
golang 1.19	2023-09-30
golang 1.9	2018-12-14
ha proxy 2	
httpd_modules	

Nome aggiuntivo	Data obsoleta
java-openjdk11	2024-09-30
kernel-5.10	
kernel-5.15	
kernel-5.4	
kernel-ng	2022-08-08
lampada - mariadb 10.2 - php 7.2	2020-11-30
ufficio libero	
patch dal vivo	
lustro	
lustro 2.10	
lynis	
mariadb10.5	2025-06-24
mate-desktop1.x	
memcached1.5	
finto	
finto 2	
mono	
nano	2018-11-14
nginx 1	
nginx 1.12	2019-09-20

Nome aggiuntivo	Data obsoleta
nginx 1.22.1	
php 7.1	2020-01-15
php 7.2	2020-11-30
php 7.3	2021-12-06
php 7.4	2022-11-03
php 8.0	2023-11-26
php 8.1	2025-12-31
php 8.2	
postgresql10	2023-09-30
postgresql11	2023-11-09
postgresql12	2024-11-14
postgresql13	2025-11-13
postgresql14	
postgresql 9.6	2022-08-09
python3	2018-08-22
python3.8	2024-10-14
rosso 4.0	2021-05-25
redis6	2026-01-31
rubino 2.4	2020-08-27
rubino 2.6	2023-03-31

Nome aggiuntivo	Data obsoleta
rubino 3.0	2024-03-31
ruggine 1	2025-05-01
selinux-ng	
calamaro 4	2023-09-30
test	
tomcat 8.5	2024-03-31
tomcat 9	
non associato 1.13	2025-05-01
non associato 1.17	
vim	2018-11-14

AL2 Utenti e gruppi riservati

AL2 prealloca determinati utenti e gruppi sia durante il provisioning dell'immagine che durante l'installazione di determinati pacchetti. Gli utenti, i gruppi e i relativi UIDs annunci GIDs sono elencati qui per evitare conflitti.

Argomenti

Elenco di utenti riservati di Amazon Linux 2

Elencato per UID

Nome utente	UID
root	0
bin	1
daemon	2
adm	3
lp	4
sincronizzare	5
shutdown	6
fermare	7
posta	8
uucp	10
operatore	11
giochi	12

Nome utente	UID
ftp	14
profilo	16
piusatore	17
calamaro	23
denominato	25
postgres	26
mysql	27
nscd	28
nscd	28
utente rpc	29
rpc	32
un backup e un backup	33
ntp	38
postino	41
gsm	42
posta null	47
apache	48
smmsp	51
gatto	53
ldap	55

Nome utente	UID
tss	59
nslcd	65
pegaso	66
avahi	70
tcpdump	72
sshd	74
radvd	75
Cyrus	76
orologio da polso	77
fax	78
dbus	81
postfix	89
quagga	92
raggio	95
raggio usd	95
hsqldb	96
colombaia	97
identico	98
nessuno	99
qemu	107

Nome utente	UID
usbmud	113
stap-server	155
avahi-autoipd	170
impulso	171
art kit	172
dhcpd	177
sanlock	179
haproxy	188
un ammasso	189
systemd-journal-gateway	191
rete sistema-d	192
sistema-d-resolve	193
uuid	357
codolo	358
stapdev	359
stafilococco	360
stafilococco	361
systemd-journal-upload	362
systemd-journal-remote	363
sabbiato	364

Nome utente	UID
pesigare	365
pcpqa	366
pz	367
memcached	368
ipsilon	369
ipapi	370
proxy kdc	371
od	372
sssd	373
lustro	374
feudi	375
tortora nullo	376
coronato	377
forcella	378
vongole può	379
clamoroso	380
clamupdate	381
colori	382
geoclue	383
aws-kinesis-agent-user	384

Nome utente	UID
agente cw	385
sciolto	386
gentile	387
saslauth	388
dirsrv	389
chrony	996
ec2-instance-connect	997
rngd	998
libstoragemgmt	999
utente ec2	1000
nfs nessuno	65534

Elencato per nome

Nome utente	UID
adm	3
un backup e un backup	33
apache	48
orologio Arp	77
avahi	70
avahi-autoipd	170

Nome utente	UID
aws-kinesis-agent-user	384
bin	1
chrony	996
clamoroso	380
vongole possono	379
aggiornamento del clam	381
forcella	378
colori	382
coronato	377
agente cw	385
Cyrus	76
daemon	2
dbus	81
dhcpd	177
dirsrv	389
colombaia	97
tortora nullo	376
ec2-instance-connect	997
utente ec2	1000
fax	78

Nome utente	UID
feudi	375
ftp	14
giochi	12
gdm	42
geoclue	383
lustro	374
ammasso	189
fermare	7
haproxy	188
hsqldb	96
ident	98
ipapi	370
ipsilon	369
proxy kdc	371
ldap	55
libstoragemgmt	999
lp	4
posta	8
postino	41
posta null	47

Nome utente	UID
memcached	368
mysql	27
denominato	25
nfs nessuno	65534
nessuno	99
nscd	28
nscd	28
nslcd	65
ntp	38
od	372
operatore	11
profilo	16
pcp	367
pcpqa	366
pegaso	66
pesigare	365
spiffero	17
educato	387
postfix	89
postgres	26

Nome utente	UID
impulso	171
qemu	107
quagga	92
raggio	95
raggio usd	95
radvd	75
rngd	998
root	0
rpc	32
utente rpc	29
rtkit	172
sabbiato	364
sanlock	179
saslauth	388
shutdown	6
smmsp	51
calamaro	23
sshd	74
sssd	373
stap-server	155

Nome utente	UID
stapdev	359
stafilococco	360
stafilococco	361
sincronizzare	5
systemd-journal-gateway	191
systemd-journal-remote	363
systemd-journal-upload	362
systemd-network	192
sistema-d-resolve	193
codolo	358
tcpdump	72
gatto	53
tss	59
sciolto	386
usb muxd	113
uucp	10
uuid	357

Elenco dei gruppi riservati di Amazon Linux 2

Elencato da GID

Group name (Nome gruppo)	GID
root	0
bin	1
daemon	2
sys	3
adm	4
tenta	5
disco	6
disco	6
lp	7
mem	8
kmem	9
ruota	10
cdrom	11
posta	12
uucp	14
man	15
profilo	16
piusatore	17
dialout	18
floppy	19

Group name (Nome gruppo)	GID
giochi	20
slocare	21
utmp	22
calamaro	23
denominato	25
postgres	26
mysql	27
nscd	28
nscd	28
utente rpc	29
rpc	32
registrare	33
registrare	33
utempter	35
kvm	36
ntp	38
video	39
tuffo	40
postino	41
gsm	42

Group name (Nome gruppo)	GID
posta null	47
apache	48
ftp	50
smmsp	51
gatto	53
serratura	54
ldap	55
tss	59
audio	63
pegaso	65
avahi	70
tcpdump	72
sshd	74
radvd	75
saslauth	76
saslauth	76
orologio da polso	77
fax	78
dbus	81
screen	84

Group name (Nome gruppo)	GID
quaggavt	85
wbpriv	88
wbpriv	88
postfix	89
postconsegna	90
quagga	92
raggio	95
raggio usd	95
hsqldb	96
colombaia	97
identità	98
nessuno	99
utenti	100
qemu	107
usbmud	113
stap-server	155
staffa	156
stafilococco	156
stapsys	157
stapdev	158

Group name (Nome gruppo)	GID
avahi-autoipd	170
impulso	171
art kit	172
dhcpd	177
sanlock	179
haproxy	188
un cliente	189
systemd-journal	190
sistema-diario	190
systemd-journal-gateway	191
rete sistema-d	192
sistema-d-resolve	193
convocazione	351
wireshark	352
uuid	353
codolo	354
systemd-journal-upload	355
sfcb	356
systemd-journal-remote	356
sabbiato	357

Group name (Nome gruppo)	GID
pegno	358
ppm	359
pz	360
memcached	361
login virtuale	362
ipsilon	363
immagini 11	364
ipapi	365
proxy kdc	366
baccelli	367
sssd	368
libvirt	369
lustro	370
feudi	371
tortuoso	372
docker	373
coronato	374
forcella	375
vongole	376
clamoroso	377

Group name (Nome gruppo)	GID
gruppo di virus	378
gruppo di virus	378
gruppo di virus	378
aggiornamento del clam	379
colori	380
geoclue	381
admin di stampa	382
aws-kinesis-agent-user	383
agente cw	384
impulso-rt	385
accesso a impulsi	386
sciolto	387
gentile	388
dirsrv	389
cgred	993
chrony	994
ec2-instance-connect	995
rngd	996
libstoragemgmt	997
ssh_keys	998

Group name (Nome gruppo)	GID
input	999
utente ec2	1000
nfs nessuno	65534

Elencato per nome

Group name (Nome gruppo)	GID
adm	4
apache	48
orologio da polso	77
audio	63
avahi	70
avahi-autoipd	170
aws-kinesis-agent-user	383
bin	1
cdrom	11
cgred	993
chrony	994
clamoroso	377
vongole possono	376
aggiornamento del clam	379

Group name (Nome gruppo)	GID
forcella	375
colori	380
coronato	374
agente cw	384
daemon	2
dbus	81
dhcpd	177
dialout	18
tuffo	40
dirsrv	389
disco	6
disco	6
docker	373
colombaia	97
tortora nullo	372
ec2-instance-connect	995
utente ec2	1000
fax	78
feudi	371
floppy	19

Group name (Nome gruppo)	GID
ftp	50
giochi	20
gdm	42
geoclue	381
lustro	370
un cliente	189
haproxy	188
hsqldb	96
ident	98
input	999
ipapi	365
ipsilon	363
proxy kdc	366
meme	9
kvm	36
ldap	55
libstoragemgmt	997
libvirt	369
serratura	54
lp	7

Group name (Nome gruppo)	GID
posta	12
postino	41
posta null	47
man	15
mem	8
memcached	361
mysql	27
denominato	25
nfs nessuno	65534
nessuno	99
nscd	28
nscd	28
ntp	38
od	367
profilo	16
pcp	360
pcpa	359
pegaso	65
pesigare	358
immagini 11	364

Group name (Nome gruppo)	GID
spizzatore	17
educato	388
postconsegna	90
postfix	89
postgres	26
admin di stampa	382
impulso	171
accesso a impulsi	386
impulso-rt	385
qemu	107
quagga	92
quaggavt	85
raggio	95
raggio usd	95
radvd	75
rngd	996
root	0
rpc	32
utente rpc	29
rtkit	172

Group name (Nome gruppo)	GID
sabbiato	357
sanlock	179
saslauth	76
saslauth	76
screen	84
sfcb	356
sloccare	21
smmsp	51
calamaro	23
ssh_keys	998
sshd	74
sssd	368
stap-server	155
stapdev	158
stafilococco	157
staffa	156
stafilococco	156
dice	3
systemd-journal	190
sistema-diario	190

Group name (Nome gruppo)	GID
systemd-journal-gateway	191
systemd-journal-remote	356
systemd-journal-upload	355
rete sistema-d	192
sistema-d-resolve	193
codolo	354
registrare	33
registrare	33
tcpdump	72
gatto	53
tss	59
tenta	5
sciolto	387
convocazione	351
usb muxd	113
utenti	100
utempter	35
utmp	22
uucp	14
uuid	353

Group name (Nome gruppo)	GID
video	39
login virt	362
gruppo di virus	378
gruppo di virus	378
gruppo di virus	378
wbpriv	88
wbpriv	88
ruota	10
wireshark	352

AL2 Pacchetti sorgente

Puoi visualizzare l'origine dei pacchetti installati sull'istanza per riferimento utilizzando gli strumenti disponibili in Amazon Linux. I pacchetti di origine sono disponibili per tutti i pacchetti inclusi in Amazon Linux e nell'archivio di pacchetti online. Determina il nome del pacchetto sorgente che desideri installare e usa il yumdownloader --source comando per visualizzare il codice sorgente all'interno dell'istanza in esecuzione. Esempio:

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

L'RPM di origine può essere decompresso e, come riferimento, è possibile visualizzare l'albero dei sorgenti utilizzando strumenti RPM standard. Dopo aver completato il debug, il pacchetto è disponibile per l'utilizzo.

Sicurezza e conformità in AL2

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWSti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWSProgrammi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano alla norma AL2 023, consulta AWSServizi compresi nell'ambito del programma di conformità AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Attiva la modalità FIPS AL2

Questa sezione spiega come abilitare gli standard federali di elaborazione delle informazioni (FIPS) su. AL2 Per ulteriori informazioni sul FIPS, consulta:

- Federal Information Processing Standard (FIPS)
- Conformità FAQs: Standard federali per l'elaborazione delle informazioni

Prerequisiti

- Un' EC2 istanza AL2 Amazon esistente con accesso a Internet per scaricare i pacchetti richiesti. Per ulteriori informazioni sul lancio di un' EC2 istanza AL2 Amazon, consultaAL2 su Amazon EC2.
- Devi connetterti alla tua EC2 istanza Amazon tramite SSH oAWS Systems Manager.

> **Important**
>
> ED25519 Le chiavi utente SSH non sono supportate in modalità FIPS. Se hai avviato l' EC2 istanza Amazon utilizzando una coppia di chiavi ED25519 SSH, devi generare nuove chiavi utilizzando un altro algoritmo (come RSA) o potresti perdere l'accesso all'istanza dopo aver abilitato la modalità FIPS. Per ulteriori informazioni, consulta Create key pair nella Amazon EC2 User Guide.

Abilitazione della modalità FIPS

1. Connect alla propria AL2 istanza tramite SSH oAWS Systems Manager.
2. Verifica che il sistema sia aggiornato. Per ulteriori informazioni, consulta Archivio dei pacchetti.
3. Installa e abilita il `dracut-fips` modulo eseguendo i seguenti comandi.

   ```
   sudo yum -y install dracut-fips
   sudo dracut -f
   ```

4. Abilita la modalità FIPS sulla riga di comando del kernel Linux usando il seguente comando. Ciò abiliterà la modalità FIPS a livello di sistema per i moduli elencati nelle domande frequenti AL2

   ```
   sudo /sbin/grubby --update-kernel=ALL --args="fips=1"
   ```

5. Riavvia l'istanza. AL2

   ```
   sudo reboot
   ```

6. Per verificare che la modalità FIPS sia abilitata, riconnettiti all'istanza ed esegui il comando seguente.

   ```
   sysctl crypto.fips_enabled
   ```

   Verrà visualizzato l'output seguente:

   ```
   crypto.fips_enabled = 1
   ```

   È inoltre possibile verificare che OpenSSH sia in modalità FIPS eseguendo il comando seguente:

```
ssh localhost 2>&1 | grep FIPS
```

Verrà visualizzato l'output seguente:

```
FIPS mode initialized
```

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.