aws

Guida per l'utente

Amazon Linux 2023

Amazon Linux 2023: Guida per l'utente

Table of Contents

Cos'è Amazon Linux 2023?

Amazon Linux 2023 (AL2023) è la nuova generazione di Amazon Linux di Amazon Web Services (AWS). Con AL2023, puoi sviluppare ed eseguire applicazioni cloud e aziendali in un ambiente di runtime sicuro, stabile e ad alte prestazioni. Inoltre, ottieni un ambiente applicativo che offre supporto a lungo termine con accesso alle ultime innovazioni in Linux. AL2023 è disponibile senza costi aggiuntivi.

AL2023 è il successore di Amazon Linux 2 (AL2). Per informazioni sulle differenze tra AL2023 e AL2, vedere e Confronto tra AL2 e AL2023 Package changes in AL2023.

Argomenti

Cadenza di rilascio

Una nuova versione principale di Amazon Linux viene rilasciata ogni due anni e include cinque anni di supporto. Ogni rilascio include il supporto in due fasi. La fase di supporto standard copre i primi due anni. Quindi, una fase di manutenzione prosegue il supporto per altri tre anni.

Nella fase di supporto standard, il rilascio riceve aggiornamenti trimestrali delle versioni minori. Durante la fase di manutenzione, un rilascio riceve solo aggiornamenti di sicurezza e correzioni di bug critici che vengono pubblicati non appena sono disponibili.

Anno	Amazon Linux 2023	Amazon Linux 2025	Amazon Linux 2027	Amazon Linux 2029
2023	Supporto standard 			
2024	Supporto standard 			
2025	Maintenance (Manutenzione)	Supporto standard 		
2026	Maintenance (Manutenzione)	Supporto standard 		
2027	Maintenance (Manutenzione)	Maintenance (Manutenzione)	Supporto standard 	
2028	EOL 	Maintenance (Manutenzione)	Supporto standard 	

Anno	Amazon Linux 2023	Amazon Linux 2025	Amazon Linux 2027	Amazon Linux 2029
2029	EOL 	Maintenance (Manutenzione)	Maintenance (Manutenzione)	Supporto standard 
2030	EOL 	EOL 	Maintenance (Manutenzione)	Supporto standard 
2031	EOL 	EOL 	Maintenance (Manutenzione)	Maintenance (Manutenzione)

Rilasci principali e secondari

Con ogni rilascio di Amazon Linux (versione principale, versione secondaria o rilascio di sicurezza), rilasciamo una nuova Amazon Machine Image (AMI) Linux.

- Rilascio di versione principale: include nuove funzionalità e miglioramenti in termini di sicurezza e prestazioni in tutto lo stack. I miglioramenti potrebbero includere importanti modifiche al kernel, alla toolchain, a Glib C, a OpenSSL e a qualsiasi altra libreria e utilità di sistema. I rilasci principali di Amazon Linux sono basati in parte sulla versione attuale della distribuzione upstream di Fedora Linux. AWS potrebbe aggiungere o sostituire pacchetti specifici da altre versioni upstream non Fedora.
- Rilascio di versione secondaria: aggiornamento trimestrale che include aggiornamenti di sicurezza, correzioni di bug, e nuove funzionalità e pacchetti. Ogni versione secondaria è un elenco cumulativo di aggiornamenti che include correzioni di sicurezza e bug oltre a nuove funzionalità e pacchetti. Questi rilasci potrebbero includere i runtime del linguaggio più recenti, come ad esempio PHP. Potrebbero includere anche altri noti pacchetti software come Ansible e Docker.

Utilizzo dei nuovi rilasci

Gli aggiornamenti vengono forniti tramite una combinazione di nuovi rilasci di Amazon Machine Image (AMI) e dei nuovi repository corrispondenti. Per impostazione predefinita, una nuova AMI e il repository a cui essa punta sono abbinati. Tuttavia, puoi indirizzare le istanze Amazon EC2 in esecuzione a versioni di repository più recenti nel corso del tempo per applicare gli aggiornamenti sulle istanze in esecuzione. Puoi eseguire l'aggiornamento anche avviando nuove istanze delle AMI più recenti.

Policy di supporto a lungo termine

Amazon Linux fornisce aggiornamenti per tutti i tuoi pacchetti e mantiene la compatibilità all'interno di una versione principale per le applicazioni basate su Amazon Linux. I pacchetti principali come la libreria glibc, OpenSSL, OpenSSH e lo strumento di gestione dei pacchetti DNF ricevono supporto per tutta la durata di validità del rilascio principale di AL2023. I pacchetti che non sono inclusi tra quelli principali sono supportati in base alle rispettive origini upstream specifiche. Puoi visualizzare lo stato e le date di supporto specifici dei singoli pacchetti eseguendo il comando seguente.

```
$ sudo dnf supportinfo --pkg packagename
```

Mediante l'esecuzione del comando riportato di seguito puoi ottenere informazioni su tutti i pacchetti attualmente installati.

```
$ sudo dnf supportinfo --show installed
```

L'elenco completo dei pacchetti principali viene finalizzato durante l'anteprima. Se vuoi visualizzare altri pacchetti inclusi tra quelli principali, non esitare a contattarci. Valutiamo mentre raccogliamo feedback. Il feedback su AL2023 può essere fornito tramite il rappresentante AWS designato o inviando un issue nel repository amazon-linux-2023 su GitHub.

Denominazione e controllo delle versioni

AL2023 fornisce una versione minore ogni tre mesi durante i due anni di supporto standard. Ogni rilascio è identificato tramite un incremento da 0 a N. 0 si riferisce al rilascio principale originale dell'iterazione in questione. Tutti i rilasci si chiameranno Amazon Linux 2023. Quando Amazon Linux 2025 verrà rilasciato, AL2023 usufruirà del supporto esteso e riceverà aggiornamenti per la sicurezza e le correzioni di bug critici.

Ad esempio, i rilasci secondari di AL2023 hanno il seguente formato:

- `2023.`**`0`**`.20230301`
- `2023.`**`1`**`.20230601`
- `2023.`**`2`**`.20230901`

Le AMI AL2023 corrispondenti hanno il formato seguente:

- `al2023-ami-2023.`**`0`**`.20230301.0-kernel-6.1-x86_64`
- `al2023-ami-2023.`**`1`**`.20230601.0-kernel-6.1-x86_64`
- `al2023-ami-2023.`**`2`**`.20230901.0-kernel-6.1-x86_64`

All'interno di una versione secondaria specifica, i rilasci periodici delle AMI avvengono con un timestamp della data di rilascio di ciascuna AMI.

- `al2023-ami-2023.0.`**`20230301`**`.0-kernel-6.1-x86_64`
- `al2023-ami-2023.0.`**`20230410`**`.0-kernel-6.1-x86_64`
- `al2023-ami-2023.0.`**`20230520`**`.0-kernel-6.1-x86_64`

Il metodo consigliato per identificare un'istanza AL2 o AL2023 inizia con la lettura della stringa Common Platform Enumeration (CPE) da. `/etc/system-release-cpe` Quindi, si suddivide la stringa nei relativi campi. Infine, leggi i valori della piattaforma e della versione.

AL2023 introduce anche nuovi file per l'identificazione della piattaforma:

- `/etc/amazon-linux-release` crea symlink a `/etc/system-release`
- `/etc/amazon-linux-release-cpe` crea symlink a `/etc/system-release-cpe`

Questi due file indicano che un'istanza è Amazon Linux. Non è necessario leggere un file o suddividere la stringa in campi a meno che non si desideri conoscere i valori specifici della piattaforma e della versione.

Ottimizzazioni relative a operazioni e prestazioni

Kernel Amazon Linux 6.1

- AL2023 utilizza i driver più recenti per i dispositivi Elastic Network Adapter (ENA) ed Elastic Fabric Adapter (EFA). AL2023 si concentra sui backport di prestazioni e funzionalità per l'hardware nell'infrastruttura Amazon EC2.
- L'applicazione di patch live del kernel è disponibile per i tipi di istanza `x86_64` e `aarch64`. In tal modo si riduce la necessità di riavviare frequentemente.
- Tutte le configurazioni di build e runtime del kernel includono molte delle stesse ottimizzazioni prestazionali e operative di AL2.

Selezione della toolchain di base e flag di build predefiniti

- I pacchetti AL2023 sono creati con le ottimizzazioni del compilatore () abilitate per impostazione predefinita `-O2`
- I pacchetti AL2023 sono sviluppati richiedendo `x86-64v2` per i sistemi `x86-64` (`-march=x86-64-v2`) e Graviton2 o versioni successive per `aarch64` (`-march=armv8.2-a+crypto -mtune=neoverse-n1`).
- I pacchetti AL2023 sono sviluppati con la vettorizzazione automatica abilitata (`-ftree-vectorize`).
- I pacchetti AL2023 sono sviluppati con la funzionalità Link Time Optimization (LTO) abilitata.
- AL2023 usa le versioni aggiornate di Rust, Clang/LLVM e Go.

Selezione e versioni dei pacchetti

- Alcuni backport per i principali componenti di sistema includono diversi miglioramenti delle prestazioni per l'esecuzione sull'infrastruttura Amazon EC2, in particolare per le istanze Graviton.
- AL2023 è integrato con diverse funzionalità. Servizi AWS Ciò include SSM Agent, Amazon Kinesis Agent e. AWS CLI CloudFormation
- AL2023 usa Amazon Corretto come Java Development Kit (JDK).
- AL2023 fornisce motori di database e aggiornamenti di runtime del linguaggio di programmazione alle versioni più recenti man mano che vengono rilasciate dai progetti upstream. I runtime del linguaggio di programmazione con nuove versioni vengono aggiunti quando vengono rilasciati.

Implementazione in un ambiente cloud

- L'AMI AL2023 di base e le immagini di container vengono aggiornate frequentemente per supportare la sostituzione delle istanze di patch.
- Gli aggiornamenti del kernel sono inclusi negli aggiornamenti AMI AL2023. Ciò significa che non è necessario utilizzare comandi come `yum update` e `reboot` per aggiornare il kernel.
- Oltre all'AMI AL2023 standard, sono disponibili anche un'immagine AMI e un'immagine di container minime. Scegli l'AMI minima per eseguire un ambiente con il numero minimo di pacchetti necessari per eseguire il servizio.
- Per impostazione predefinita, le AMI e i container di AL2023 sono collegati a una versione specifica dei repository di pacchetti. Non è previsto alcun aggiornamento automatico all'avvio. Ciò significa che hai sempre il controllo su quando importare eventuali aggiornamenti dei pacchetti. Puoi sempre eseguire i test in un ambiente beta/gamma prima di passare alla produzione. Se c'è un problema, puoi usare il percorso di rollback preconvalidato.

Relazione con Fedora

AL2023 mantiene i propri cicli di vita di rilascio e supporto indipendenti da Fedora. AL2023 fornisce versioni aggiornate del software open source, una più ampia varietà di pacchetti e rilasci frequenti. In questo modo vengono preservati i familiari sistemi operativi basati su RPM.

La versione disponibile a livello generale (GA) di AL2023 non è direttamente paragonabile a nessuna versione specifica di Fedora. La versione GA di AL2023 include componenti di Fedora 34, 35 e 36. Alcuni componenti sono identici a quelli di Fedora e altri sono stati modificati. Altri componenti assomigliano di più ai componenti di CentOS 9 Stream o sono stati sviluppati in modo indipendente. Il kernel Amazon Linux proviene dalle opzioni di supporto a lungo termine disponibili su kernel.org, scelte indipendentemente da Fedora.

cloud-init personalizzato

Il pacchetto cloud-init è un'applicazione open source che esegue il bootstrap delle immagini Linux in un ambiente di cloud computing. Per ulteriori informazioni, consulta la documentazione di cloud-init.

AL2023 contiene una versione personalizzata di cloud-init. Con cloud-init, puoi specificare ciò che accade all'istanza in fase di avvio.

Quando avvii un'istanza, puoi utilizzare i campi di dati utente a cui passare azioni. cloud-init Ciò significa che puoi utilizzare le Amazon Machine Image (AMI) comuni per numerosi casi d'uso e configurarle in modo dinamico quando avvii un'istanza. AL2023 utilizza anche cloud-init per configurare l'account `ec2-user`.

AL2023 utilizza le azioni cloud-init in `/etc/cloud/cloud.cfg.d` e `/etc/cloud/cloud.cfg`. Puoi creare file di azioni cloud-init personalizzato nella directory `/etc/cloud/cloud.cfg.d`. Cloud-init legge tutti i file in questa directory in ordine lessicografico. I file più recenti sovrascrivono i valori dei file meno recenti. Quando cloud-init avvia un'istanza, il pacchetto cloud-init esegue le seguenti attività di configurazione:

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

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

    Per un maggiore controllo sui montaggi, consulta la pagina dedicata ai montaggi nella documentazione di cloud-init.

- All'avvio di un'istanza, i volumi dell'archivio dell'istanza che supportano TRIM non vengono formattati. Prima di poter montare i volumi dell'archivio dell'istanza, è necessario partizionare e formattare i relativi volumi.

  Per ulteriori informazioni, consulta la pagina dedicata al supporto TRIM dei volumi dell'archivio dell'istanza nella Guida per l'utente di Amazon EC2 per le istanze Linux.
- All'avvio delle istanze, è possibile utilizzare il modulo `disk_setup` per partizionare e formattare i volumi dell'archivio dell'istanza.

  Per ulteriori informazioni, consulta la pagina dedicata alla configurazione disco nella documentazione di cloud-init.

Per ulteriori informazioni sull'uso di cloud-init con SELinux, consulta Uso di cloud-init per abilitare la modalità `enforcing`.

Per informazioni sui formati dei dati utente cloud-init, consulta la pagina dedicata ai formati dei dati utente nella documentazione di cloud-init.

Aggiornamenti e funzionalità di sicurezza

AL2023 fornisce molti aggiornamenti e soluzioni di sicurezza.

Argomenti

- Gestione degli aggiornamenti
- Sicurezza nel cloud
- modalità di SELinux
- Programma di conformità
- server SSH predefinito
- Funzionalità principali di OpenSSL 3

Gestione degli aggiornamenti

Applica gli aggiornamenti di sicurezza utilizzando DNF le versioni del repository. Per ulteriori informazioni, consulta Gestione degli aggiornamenti dei pacchetti e del sistema operativo in AL2023.

Sicurezza nel cloud

La sicurezza è una responsabilità condivisa tra te AWS e te. Il modello di responsabilità condivisa lo descrive come sicurezza del cloud e sicurezza nel cloud. Per ulteriori informazioni, consulta Sicurezza e conformità in Amazon Linux 2023.

modalità di SELinux

Per impostazione predefinita, SELinux è abilitato e impostato sulla modalità di autorizzazione in AL2023. In modalità di autorizzazione, le negazioni di autorizzazione vengono registrate ma non applicate.

Le policy SELinux definiscono le autorizzazioni per utenti, processi, programmi, file e dispositivi. Con SELinux, puoi scegliere una delle due policy. Le policy sono mirate o di sicurezza multilivello (MLS).

Per ulteriori informazioni sulle modalità e le policy di SELinux, consulta Impostazione delle modalità SELinux per AL2023 e la pagina wiki del progetto SELinux.

Programma di conformità

Revisori indipendenti valutano la sicurezza e la conformità di AL2023 insieme a molti programmi di AWS conformità.

server SSH predefinito

AL2023 include OpenSSH 8.7. OpenSSH 8.7 disabilita per impostazione predefinita l'algoritmo di scambio delle chiavi `ssh-rsa`. Per ulteriori informazioni, consulta Configurazione del server SSH predefinita.

Funzionalità principali di OpenSSL 3

- Il Certificate Management Protocol (CMP, RFC 4210) include sia il protocollo CRMF (RFC 4211) che il protocollo di trasferimento HTTP (RFC 6712).
- Un client HTTP o HTTPS in libcrypto supporta le azioni GET e POST, il reindirizzamento, i contenuti di testo semplice e con codifica ASN.1, i proxy e i timeout.
- EVP_KDF è compatibile con le funzioni di derivazione delle chiavi.
- EVP_MAC API è compatibile con MACs.
- Supporto TLS per il kernel Linux.

Per ulteriori informazioni, consulta la guida per la migrazione a OpenSSL.

Servizio di networking

Il progetto `systemd-networkd` open source è disponibile a livello esteso nelle moderne distribuzioni Linux. Il progetto usa un linguaggio di configurazione dichiarativo simile al resto del framework `systemd`. I relativi tipi di file di configurazione principali sono i file `.network` e `.link`.

Il pacchetto `amazon-ec2-net-utils` genera configurazioni specifiche dell'interfaccia nella directory `/run/systemd/network`. Queste configurazioni abilitano le reti IPv4 e IPv6 sulle interfacce quando sono collegate a un'istanza. Queste configurazioni installano anche regole di instradamento delle policy che aiutano a garantire che il traffico con origine locale venga instradato alla rete attraverso l'interfaccia di rete dell'istanza corrispondente. Queste regole garantiscono che il traffico corretto venga instradato attraverso l'Elastic Network Interface (ENI) dagli indirizzi o dai prefissi associati. Per ulteriori informazioni sull'uso di ENI, consulta la pagina dedicata nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Puoi personalizzare questo comportamento di rete inserendo un file di configurazione personalizzato nella directory `/etc/systemd/network` per sovrascrivere le impostazioni di configurazione predefinite contenute in `/run/systemd/network`.

La documentazione di systemd.network descrive in che modo il servizio `systemd-networkd` determina la configurazione da applicare a un'interfaccia specifica. Genera anche nomi alternativi, noti comealtnames, per le interfacce supportate da ENI per riflettere le proprietà di varie risorse. AWS Queste proprietà delle interfacce supportate da ENI sono il campo `ENI ID` e `DeviceIndex` del collegamento ENI. Puoi fare riferimento a queste interfacce utilizzando le relative proprietà quando si utilizzano vari strumenti, come il comando `ip`.

I nomi delle interfacce di istanza AL2023 vengono generati utilizzando lo schema di denominazione degli slots`systemd`. Per ulteriori informazioni, consulta lo schema di denominazione systemd.net.

Inoltre, AL2023 usa per impostazione predefinita l'algoritmo di pianificazione della trasmissione di rete per la gestione delle code attive `fq_codel`. Per ulteriori informazioni, vedere CoDel panoramica.

Pacchetti di toolchain principali glibc, gcc, binutils

Un sottoinsieme di pacchetti in Amazon Linux sono designati come pacchetti toolchain principali. Come parte principale di AL2023, i pacchetti principali ricevono cinque anni di supporto. Potremmo

cambiare la versione di un pacchetto, ma il supporto a lungo termine si applica al pacchetto incluso nel rilascio di Amazon Linux.

Questi tre pacchetti principali forniscono una toolchain di sistema che viene utilizzata per sviluppare la maggior parte del software nella distribuzione Amazon Linux.

Pacchetto	Definizione	Scopo
glibc 2.34	Libreria di sistema C	Utilizzata dalla maggior parte dei programmi binari che forniscono funzioni standard e dall'interfaccia tra i programmi e il kernel.
gcc 11.2	Suite di compilatori gcc	Compila C, C++, Fortran.
binutils 2.35	Assembler e linker più altri strumenti binari	Manipola o ispeziona i programmi binari.

Consigliamo di far seguire gli aggiornamenti applicati a tutte le librerie glibc 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.

Strumento di gestione dei pacchetti

Lo strumento di gestione dei pacchetti software predefinito in AL2023 è. DNF DNFè il successore dello strumento di YUM gestione dei pacchetti di AL2.

DNF è simile a YUM in termini di utilizzo. Molti DNF comandi e opzioni di comando sono uguali ai comandiYUM. In un comando dell'interfaccia a riga di comando (CLI), nella maggior parte dei casi `dnf` sostituisce `yum`.

Ad esempio, per i seguenti `yum` comandi AL2:

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

In AL2023, diventano i seguenti comandi:

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

In AL2023 il comando `yum` è ancora disponibile, ma come puntatore al comando `dnf`. Quindi, quando il comando `yum` viene utilizzato nella shell o in uno script, tutti i comandi e le opzioni sono gli stessi di DNF CLI. Per ulteriori informazioni sulle differenze tra YUM CLI e DNF CLI, consulta la pagina dedicata alle modifiche apportate in DNF CLI rispetto a YUM.

Per un riferimento completo dei comandi e delle opzioni per il comando `dnf`, consulta la pagina man di `man dnf`. Per ulteriori informazioni, vedere DNFCommand Reference.

Configurazione del server SSH predefinita

Se disponi di client SSH risalenti a diversi anni fa, potresti visualizzare un errore quando ti connetti a un'istanza. Se l'errore indica che non è stato trovato alcun tipo di chiave host corrispondente, aggiorna la chiave host SSH per risolvere il problema.

Disabilitazione predefinita delle firme **`ssh-rsa`**

AL2023 include una configurazione predefinita che disabilita l'algoritmo della chiave `ssh-rsa` host legacy e genera un set ridotto di chiavi host. I client devono supportare `ssh-ed25519` o l'algoritmo delle chiavi host `ecdsa-sha2-nistp256`.

La configurazione predefinita accetta uno qualsiasi di questi algoritmi di scambio delle chiavi:

- `curve25519-sha256`
- `curve25519-sha256@libssh.org`
- `ecdh-sha2-nistp256`
- `ecdh-sha2-nistp384`
- `ecdh-sha2-nistp521`
- `diffie-hellman-group-exchange-sha256`
- `diffie-hellman-group14-sha256`
- `diffie-hellman-group16-sha512`
- `diffie-hellman-group18-sha512`

Per impostazione predefinita, AL2023 genera le chiavi host `ed25519` e `ECDSA`. I client supportano `ssh-ed25519` o l'algoritmo delle chiavi host `ecdsa-sha2-nistp256`. Quando ti connetti tramite SSH a un'istanza, devi usare un client che supporti un algoritmo compatibile, ad esempio `ssh-ed25519` o `ecdsa-sha2-nistp256`. Se devi usare altri tipi di chiave, sostituisci l'elenco delle chiavi generate con un frammento `cloud-config` nei dati utente.

Nell'esempio seguente, `cloud-config` genera una chiave host `rsa` con le chiavi `ecdsa` e `ed25519`.

```
#cloud-config
 ssh_genkeytypes:
 - ed25519
 - ecdsa
 - rsa
```

Se usi una coppia di chiavi RSA per l'autenticazione della chiave pubblica, il client SSH deve supportare una firma `rsa-sha2-256` o `rsa-sha2-512`. Se usi un client incompatibile e non riesci a eseguire l'aggiornamento, riabilita il supporto per `ssh-rsa` nell'istanza. Per riattivare `ssh-rsa` il supporto, attiva la policy di crittografia del `LEGACY` sistema utilizzando i seguenti comandi.

```
$ sudo dnf install crypto-policies-scripts
$ sudo update-crypto-policies --set LEGACY
```

Per ulteriori informazioni sulla gestione delle chiavi host, consulta Amazon Linux Host keys.

Funzionalità obsolete in AL2023

Le funzionalità obsolete in AL2 e non presenti in AL2023 sono documentate qui. Si tratta di funzionalità come caratteristiche e pacchetti presenti in AL2, ma non in AL2023 e che non verranno aggiunte ad AL2023. Per ulteriori informazioni sulla durata del supporto della funzionalità in AL2, vedere Funzionalità obsoleta in AL2.

C'è anche una funzionalità in AL2023 che è obsoleta e verrà rimossa in una versione futura. Questo capitolo descrive cos'è questa funzionalità, quando non è più supportata e quando verrà rimossa da Amazon Linux. Comprendere le funzionalità obsolete ti aiuterà a distribuire AL2023 e a prepararti per la prossima versione principale di Amazon Linux.

Argomenti

Pacchetti **`compat-`**

Tutti i pacchetti in AL2 con il prefisso di `compat-` vengono 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) sono obsoleti 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 AL1, rimossa in AL2

Questa sezione descrive le funzionalità disponibili in AL1 e non più disponibili in 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 le istruzioni di supporto del pacchetto AL1.

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

Argomenti

AMI x86 (i686) a 32 bit

Come parte della versione 2014.09 di AL1, Amazon Linux ha annunciato che sarebbe stata l'ultima versione a produrre AMI a 32 bit. 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 i 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 ad AL2023.

Se è necessario eseguire file binari a 32 bit su AL2023, è possibile utilizzare lo spazio utente a 32 bit di AL2 all'interno di un contenitore AL2 eseguito 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 agli utenti di effettuare chiamate API Amazon EC2. AWS CLI Questi strumenti sono stati interrotti nel 2015 e sono AWS CLI diventati il modo preferito per interagire con le API di Amazon EC2 dalla riga di comando. Il set di utilità da riga di comando 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, ad esempio per fornire agli utenti `aws-apitools-ec2` la compatibilità con le versioni precedenti. AWS CLI È uno strumento più robusto e completo rispetto ai `aws-apitools-*` pacchetti in quanto viene mantenuto attivamente e fornisce un mezzo per utilizzare tutte le API. AWS

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.

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

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

AL2 è stata la prima versione di Amazon Linux a utilizzare il sistema `systemd` init, `upstart` in sostituzione di AL1. Qualsiasi configurazione `upstart` specifica deve essere modificata come parte della migrazione da AL1 a 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 AL2023.

Funzionalità obsoleta in AL2 e rimossa in AL2023

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

Argomenti

- cgroup v1
- log4jlog4j-cve-2021-44228-hotpatchhotpatch ()
- lsb_release e il pacchetto system-lsb-core
- mcrypt
- OpenJDK (7) java-1.7.0-openjdk
- Python 2.7
- rsyslog-opensslsostituisce rsyslog-gnutls

Pacchetti x86 (i686) a 32 bit

Come parte della versione 2014.09 di AL1, abbiamo annunciato che sarebbe stata l'ultima versione a produrre AMI a 32 bit. 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 di AL2 all'interno di un contenitore AL2 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 le API di Amazon EC2 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 utilizzare tutte le API. AWS

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.

`bzr`sistema di controllo delle revisioni

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

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

cgroup v1

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

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

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

In risposta a CVE-2021-44228, Amazon Linux ha rilasciato una versione in pacchetto RPM di Hotpatch per Apache Log4j per AL1 e 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 a disponibilità generale di AL2023 risale a 15 mesi dopo CVE-2021-44228, quindi AL2023 non viene fornito con l'hotpatch (abilitato o meno).

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 comando `lsb_release` (fornito in AL2 dal pacchetto `system-lsb-core`) 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 comando `lsb_release` e non include il pacchetto `system-lsb-core`. 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 l'PHPestensione 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 trasferire il proprio codice suOpenSSL, poiché non `mcrypt` verrà aggiunto ad 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 obsoleti in AL2 e non sono più presenti in AL2023. Il JDK più vecchio disponibile in AL2023 è fornito da Corretto 8.

Per ulteriori informazioni su Java su Amazon Linux, consultaJava in AL2023.

Python 2.7

> **Note**
>
> AL2023 ha rimosso Python 2.7, 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. Python in AL2023

`rsyslog-openssl`sostituisce `rsyslog-gnutls`

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

Obsoleto in AL2023

Questa sezione descrive le funzionalità presenti in AL2023 e che probabilmente verranno rimosse in una versione futura di Amazon Linux. Ogni sezione descriverà in cosa consiste la funzionalità e quando è prevista la sua rimozione da Amazon Linux.

> **Note**
>
> Questa sezione verrà aggiornata nel tempo man mano che l'ecosistema Linux si evolverà e le future versioni principali di Amazon Linux saranno più vicine al rilascio.

Argomenti

Supporto per runtime x86 (i686) a 32 bit

AL2023 mantiene la capacità di eseguire file binari x86 (i686) a 32 bit. È probabile che la prossima versione principale di Amazon Linux non supporterà più l'esecuzione di file binari con spazio utente a 32 bit.

Berkeley DB () `libdb`

AL2023 viene fornito con la versione 5.3.28 della libreria Berkeley DB (). `libdb` Questa è l'ultima versione di Berkeley DB prima che la licenza passasse alla licenza GNU Affero GPLv3 (AGPL), dalla meno restrittiva licenza Sleepycat.

Ci sono pochi pacchetti in AL2023 che dipendono ancora da Berkeley DB (`libdb`) e la libreria verrà rimossa nella prossima versione principale di Amazon Linux.

> **Note**
>
> Il gestore di `dnf` pacchetti di AL2023 mantiene il supporto di sola lettura per un database in formato Berkeley DB (BDB). `rpm` Questo supporto verrà rimosso nella prossima versione principale di Amazon Linux.

`cron`

Il pacchetto `cronie` è stato installato per impostazione predefinita sull'AMI AL2, fornendo supporto per il metodo `crontab` tradizionale di pianificazione delle attività periodiche. In AL2023, non `cronie` è incluso per impostazione predefinita. Pertanto, il supporto per non `crontab` è più fornito per impostazione predefinita.

In AL2023, è possibile installare facoltativamente il `cronie` pacchetto per utilizzare i job classici`cron`. Ti consigliamo di eseguire la migrazione ai timer `systemd` grazie alle funzionalità aggiuntive fornite da `systemd`.

È possibile che una versione futura di Amazon Linux, probabilmente la prossima versione principale, non includa più il supporto per i `cron` lavori classici e completi la transizione ai `systemd` timer. Ti consigliamo di abbandonare l'utilizzo. `cron`

IMDSv1

Per impostazione predefinita, le AMI AL2023 sono configurate per l'avvio in modalità IMDSv2 -only, disabilitando l'uso di. IMDSv1 È ancora possibile utilizzare AL2023 con iMDSv1 abilitato. È probabile che una versione futura di Amazon Linux venga applicata solo IMDSv2 -only.

Per ulteriori informazioni sulla configurazione IMDS per le AMI, consulta Configure the AMI nella Amazon EC2 User Guide for Linux Instances.

`pcre`versione 1

Il `pcre` pacchetto legacy è obsoleto e verrà rimosso nella prossima versione principale di Amazon Linux. Il pacchetto `pcre2` è il successore. Sebbene le prime versioni di AL2023 fossero fornite con un numero limitato di pacchetti integrati`pcre`, questi pacchetti verranno migrati all'interno di AL2023. `pcre2` La libreria obsoleta rimarrà disponibile in AL2023`pcre`.

> **Note**
>
> La versione obsoleta di non `pcre` riceverà aggiornamenti di sicurezza per l'intera durata di AL2023. Per ulteriori informazioni sul ciclo di vita del `pcre` supporto e sulla quantità di tempo in cui il pacchetto riceverà gli aggiornamenti di sicurezza, consulta le istruzioni di supporto del pacchetto. `pcre`

System V init (**`sysvinit`**)

Sebbene AL2023 mantenga la retrocompatibilità con gli script System V service (init), il `systemd` progetto upstream, come parte della sua versione v254, ha annunciato l'obsolescenza del supporto per gli script di servizio System V e ha indicato che il supporto verrà rimosso in una versione futura di. `systemd` Per ulteriori informazioni, consulta systemd.

AL2023 manterrà la retrocompatibilità con gli script System V service (init), ma gli utenti sono incoraggiati a migrare all'utilizzo di file `systemd` unit nativi per essere preparati alla rimozione del supporto per gli script System V service (init) da Amazon Linux, probabilmente nella prossima versione principale.

Confronto tra AL2 e AL2023

I seguenti argomenti descrivono le differenze principali tra AL2 e AL2023.

Argomenti

- Tripletta del compilatore
- Pacchetti x86 (i686) a 32 bit
- lsb_release e il pacchetto system-lsb-core
- Modifiche al kernel AL2023 rispetto a AL2
- Confronto dei pacchetti installati sulle AMI Amazon Linux 2 e Amazon Linux 2023
- Confronto dei pacchetti installati sulle AMI minime Amazon Linux 2 e Amazon Linux 2023
- Confronto dei pacchetti installati sulle immagini dei container di base Amazon Linux 2 e Amazon Linux 2023

Pacchetti aggiunti, aggiornati e rimossi

AL2023 contiene migliaia di pacchetti software disponibili per l'uso. Per un elenco completo di tutti i pacchetti aggiunti, aggiornati o rimossi in AL2023 rispetto alle versioni precedenti di Amazon Linux, consulta Modifiche apportate ai pacchetti in AL2023.

Per richiedere l'aggiunta o la modifica di un pacchetto in AL2023, segnala un problema nel repository amazon-linux-2023 su. GitHub

Supporto per ogni rilascio

Per AL2023, offriamo cinque anni di supporto.

Per ulteriori informazioni, consulta Cadenza di rilascio.

Modifiche alla denominazione e al controllo delle versioni

AL2023 supporta gli stessi meccanismi supportati da AL2 per l'identificazione della piattaforma. AL2023 introduce anche nuovi file per l'identificazione della piattaforma.

Per ulteriori informazioni, consulta Denominazione e controllo delle versioni.

Ottimizzazioni

AL2023 ottimizza i tempi di avvio per ridurre il periodo che intercorre tra l'avvio dell'istanza e l'esecuzione del carico di lavoro del cliente. Queste ottimizzazioni riguardano la configurazione

del kernel dell'istanza Amazon EC2, le configurazioni `cloud-init` e le funzionalità integrate nei pacchetti del sistema operativo come `kmod` e `systemd`.

Per ulteriori informazioni su queste ottimizzazioni, consulta Ottimizzazioni relative a operazioni e prestazioni.

Python 2.7 è stato sostituito con Python 3

AL2 fornisce supporto e patch di sicurezza per Python 2.7 fino a giugno 2025, come parte del nostro impegno di supporto a lungo termine (LTS) per i pacchetti principali di AL2. Questo supporto si estende oltre la dichiarazione della comunità Python upstream di Python end-of-life 2.7 di gennaio 2020.

AL2 usa il gestore di `yum` pacchetti, che ha una forte dipendenza da Python 2.7. In AL2023 il gestore di pacchetti `dnf` ha effettuato la migrazione a Python 3 e non richiede più Python 2.7. AL2023 è stato completamente spostato su Python 3.

> **Note**
>
> AL2023 ha rimosso Python 2.7, 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 Python in AL2023.

Aggiornamenti di sicurezza

SELinux

Per impostazione predefinita, Security Enhanced Linux (SELinux) per AL2023 è `enabled` e impostato sulla modalità `permissive`. In modalità `permissive`, le negazioni di autorizzazione vengono registrate ma non applicate.

SELinux è una funzionalità di sicurezza del kernel Amazon Linux, che era `disabled` in AL2. SELinux è una raccolta di funzionalità e utilità del kernel che fornisce l'architettura per il controllo degli accessi obbligatorio (MAC) nei principali sottosistemi del kernel.

Per ulteriori informazioni, consulta Impostazione delle modalità SELinux per AL2023.

Per ulteriori informazioni su repository, strumenti e policy di SELinux, consulta le pagine dedicate a SELinux Notebook, tipi di policy SELinux e progetto SELinux.

OpenSSL 3

AL2023 dispone del toolkit di crittografia Open Secure Sockets Layer version 3 (OpenSSL 3). AL2023 supporta i protocolli di rete TLS 1.3 e TLS 1.2.

Per impostazione predefinita, AL2 viene fornito con OpenSSL 1.0.2. Puoi sviluppare applicazioni contro OpenSSL 1.1.1.

Per ulteriori informazioni su OpenSSL, consulta la guida per la migrazione a OpenSSL.

Per ulteriori informazioni sulla sicurezza, consulta Aggiornamenti e funzionalità di sicurezza.

IMDSv2

Per impostazione predefinita, tutte le istanze avviate con l'AMI AL2023 richiedono IMDSv2 solo - only e il limite di hop predefinito sarà impostato su 2 per consentire il supporto di carichi di lavoro containerizzati. Questo è possibile impostando il parametro `imds-support` su `v2.0`. Per ulteriori informazioni, consulta la pagina che spiega come configurare l'AMI nella Guida per l'utente di Amazon EC2 per le istanze Linux.

> **Note**
>
> Il periodo di validità del token di sessione può essere compreso tra 1 secondo e 6 ore. Gli indirizzi a cui inviare le richieste API per le query IMDSv2 sono i seguenti:
>
> - IPv4: 169.254.169.254
> - IPv6: fd00:ec2::254

È possibile sovrascrivere manualmente queste impostazioni e IMDSv1 abilitarle utilizzando le proprietà di avvio dell'opzione Instance Metadata. Puoi anche utilizzare i controlli IAM per applicare impostazioni diverse. IMDS Per ulteriori informazioni sulla configurazione e l'utilizzo del servizio di metadati di istanza, consulta le pagine dedicate a utilizzo di IMDSv2, configurazione delle opzioni per i metadati di istanza per le nuove istanze e modifica delle opzioni per i metadati di istanza per le nuove istanze nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Rimozione di hotpatch log4j (`log4j-cve-2021-44228-hotpatch`)

> **Note**
>
> AL2023 non viene fornito con il pacchetto `log4j-cve-2021-44228-hotpatch`.

In risposta a CVE-2021-44228, Amazon Linux ha rilasciato una versione in pacchetto RPM di Hotpatch per Apache Log4j per AL1 e AL2. Nell'annuncio dell'aggiunta dell'hotpatch ad Amazon Linux abbiamo indicato 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 disponibile a livello generale di AL2023 risale a 15 mesi dopo CVE-2021-44228, quindi AL2023 non viene fornito con l'hotpatch (abilitato o meno).

Gli utenti che eseguono `log4j` le proprie versioni su Amazon Linux devono assicurarsi di aver effettuato l'aggiornamento alle versioni non interessate da CVE-2021-44228 o CVE-2021-45046.

AL2023 fornisce indicazioni su Aggiornamento di AL2023 in modo da restare al passo con le patch di sicurezza. Gli avvisi di sicurezza sono pubblicati nella pagina Amazon Linux Security Center.

Aggiornamenti deterministici per la stabilità

Con gli aggiornamenti deterministici tramite la funzionalità di repository con versioni, ogni AMI AL2023 per impostazione predefinita è bloccata su una versione di repository specifica. Puoi usare gli aggiornamenti deterministici per ottenere una maggiore coerenza tra gli aggiornamenti e le versioni dei pacchetti. Ogni rilascio, principale o secondario, include una versione di repository specifica.

Novità di AL2023: l'aggiornamento deterministico per impostazione predefinita è abilitato. Si tratta di un miglioramento rispetto al metodo di blocco manuale incrementale utilizzato in AL2 e in altre versioni precedenti.

Per ulteriori informazioni, consulta Utilizzo degli aggiornamenti deterministici tramite il repository con versioni su AL2023.

Origine da diversi upstream

AL2023 è basato su RPM e include componenti che hanno origine da più versioni di Fedora e altre distribuzioni, come CentOS 9 Stream. Il kernel Amazon Linux ha origine dai rilasci di supporto a lungo termine (LTS) direttamente da kernel.org, scelti indipendentemente dalle altre distribuzioni.

Per ulteriori informazioni, consulta Relazione con Fedora.

File system root AMI e tipo di volume Amazon EBS predefinito

L'AMI AL2023 e AL2 usano entrambi il file system XFS sul file system root. Per AL2023, le opzioni `mkfs` per il file system del dispositivo root sono ulteriormente ottimizzate per Amazon EC2. AL2023 supporta anche una serie di altri file system che puoi utilizzare su altri volumi per soddisfare requisiti specifici.

Le AMI AL2023 usano i volumi `gp3` di Amazon EBS per impostazione predefinita, mentre le AMI AL2 usano i volumi `gp2` di Amazon EBS per impostazione predefinita. Puoi modificare il tipo di volume quando avvii un'istanza.

Per ulteriori informazioni sui tipi di volume di Amazon EBS, consulta la pagina dedicata ai volumi per uso generale di Amazon EBS.

Per ulteriori informazioni sull'avvio di un'istanza Amazon EC2, consulta Avvio di un'istanza nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Servizio di sistema delle reti

Il servizio di sistema `systemd-networkd` gestisce le interfacce di rete in AL2023. Questa è una modifica rispetto ad AL2, che usa ISC dhclient o `dhclient`.

Per ulteriori informazioni, consulta Servizio di networking.

Gerarchia dei gruppi di controllo unificati (cgroup v2)

Un gruppo di controllo (cgroup) è una funzionalità del kernel Linux per organizzare gerarchicamente i processi e distribuire le risorse di sistema tra di essi. I gruppi di controllo vengono usati estensivamente per implementare un runtime di container e da `systemd`.

Supporta AL2 e supporta AL2023. cgroupv1 cgroupv2 Ciò è particolarmente importante se si eseguono carichi di lavoro containerizzati, ad esempio in caso di Utilizzo di AMI Amazon ECS basate su AL2023 per ospitare carichi di lavoro containerizzati.

Sebbene AL2023 includa ancora codice che può far funzionare il sistema utilizzandocgroupv1, questa non è una configurazione consigliata o supportata e verrà completamente rimossa in una futura versione principale di Amazon Linux.

Esiste un'ampia documentazione riguardante le interfacce del kernel Linux di basso livello, nonché la documentazione sulla delega systemd cgroup.

Un caso d'uso comune al di fuori dei contenitori consiste nella creazione di `systemd` unità con limiti alle risorse di sistema che possono utilizzare. Per ulteriori informazioni, vedere systemd.resource-control.

Pianificazione delle attività

Il pacchetto `cronie` è stato installato per impostazione predefinita sull'AMI AL2, fornendo supporto per il metodo `crontab` tradizionale di pianificazione delle attività periodiche. In AL2023, non è incluso per impostazione predefinita. `cronie` Pertanto, il supporto per non `crontab` è più fornito per impostazione predefinita.

Facoltativamente, è possibile installare il pacchetto `cronie` per usare i processi `cron` classici. Ti consigliamo di eseguire la migrazione ai timer `systemd` grazie alle funzionalità aggiuntive fornite da `systemd`.

Pacchetti per glibc, gcc e binutils

AL2023 include molti degli stessi pacchetti principali di AL2.

Abbiamo aggiornato i seguenti tre pacchetti di toolchain principali per AL2023.

Nome pacchetto	AL2	AL2023
glibc	2,26	2,34
gcc	7.3	11,3
binutils	2,29	2,39

Per ulteriori informazioni, consulta Pacchetti di toolchain principali glibc, gcc, binutils.

Programma di gestione dei pacchetti

Lo strumento di gestione dei pacchetti software predefinito su AL2023 è DNF. DNF è il successore di YUM, lo strumento di gestione dei pacchetti di AL2.

Per ulteriori informazioni, consulta Strumento di gestione dei pacchetti.

Sistema di registrazione di log

In AL2023 il pacchetto del sistema di registrazione di log è cambiato rispetto ad AL2. AL2023 non installa `rsyslog` per impostazione predefinita, quindi i file di log basati su testo come `/var/log/messages` che erano disponibili in AL2 non sono disponibili per impostazione predefinita. La configurazione predefinita per AL2023 è `systemd-journal`, che può essere esaminata utilizzando `journalctl`. Sebbene `rsyslog` sia un pacchetto opzionale in AL2023, consigliamo la nuova interfaccia `journalctl` basata su `systemd` basata e i pacchetti correlati. Per ulteriori informazioni, consulta la pagina del manuale di `journalctl`.

Modifiche ai pacchetti per **`curl`** e **`libcurl`**

AL2023 separa i protocolli e le funzionalità comuni dei pacchetti `curl` e `libcurl` in `curl-minimal` e `libcurl-minimal`. In questo modo è possibile ridurre l'ingombro di disco, memoria e dipendenze per la maggior parte degli utenti e si tratta del pacchetto predefinito per i container e le AMI AL2023.

Se è richiesta la piena funzionalità di `curl`, ad esempio per il supporto di `gopher://`, esegui i seguenti comandi per installare i pacchetti `curl-full` e `libcurl-full`.

```
$ dnf swap libcurl-minimal libcurl-full
```

```
$ dnf swap curl-minimal curl-full
```

GNU Privacy Guard (GNUPG)

AL2023 separa le funzionalità minime e complete per il pacchetto `gnupg2` nei pacchetti `gnupg2-minimal` e `gnupg2-full`. Per impostazione predefinita, solo il pacchetto `gnupg2-minimal` viene installato. In questo modo è possibile ottenere la funzionalità minima richiesta per verificare le firme digitali sui pacchetti `rpm`.

Per ulteriori funzionalità di `gnupg2` (ad esempio la possibilità di scaricare le chiavi da un server di chiavi), assicurati che il pacchetto `gnupg2-full` sia installato. Esegui il comando riportato di seguito per scambiare `gnupg2-minimal` e `gnupg2-full`.

```
$ dnf swap gnupg2-minimal gnupg2-full
```

Amazon Corretto come JVM predefinita

AL2023 viene fornito con Amazon Corretto come Java Development Kit (JDK) predefinito (e unico). Tutti i pacchetti Java basati in AL2023 sono tutti costruiti con. Amazon Corretto 17

Se stai migrando da AL2, puoi passare senza problemi dalla `OpenJDK` versione equivalente su AL2 a. Amazon Corretto

AWS CLI v2

AL2023 viene fornito con la AWS CLI versione 2, mentre AL2 viene fornito con la versione 1 di. AWS CLI

UEFI Preferred

Per impostazione predefinita, tutte le istanze avviate con l'AMI AL2023 su tipi di istanza che supportano il firmware UEFI vengono avviate in modalità UEFI. Questo è possibile impostando il parametro della modalità di avvio dell'AMI su `uefi-preferred`. Per ulteriori informazioni, consulta la pagina dedicata alle modalità di avvio nella Guida per l'utente di Amazon EC2 per istanze Linux.

Modifiche alla configurazione predefinita del server SSH

Per l'AMI AL2023, abbiamo cambiato i tipi delle chiavi host `sshd` che generiamo con il rilascio. Abbiamo anche eliminato alcuni tipi di chiavi legacy per evitare di generarli al momento dell'avvio. I client devono supportare i protocolli `rsa-sha2-256` e `rsa-sha2-512` oppure `ssh-ed25519` con l'uso di una chiave `ed25519`. Per impostazione predefinita, le firme `ssh-rsa` sono disabilitate.

Inoltre, le impostazioni di configurazione di AL2023 nel file `sshd_config` predefinito contengono `UseDNS=no`. Questa nuova impostazione significa che è meno probabile che eventuali problemi con DNS blocchino la capacità di stabilire sessioni `ssh` con le istanze. Come compromesso, le voci di riga `from=`*`hostname.domain`*`,`*`hostname.domain`* nei file `authorized_keys` non verranno risolte.

Poiché `sshd` non tenta più di risolvere i nomi DNS, ogni valore *`hostname.domain`* separato da virgole deve essere tradotto in un IP address corrispondente.

Per ulteriori informazioni, consulta Configurazione del server SSH predefinita.

Extra Packages for Enterprise Linux (EPEL)

Extra Packages for Enterprise Linux (EPEL) è un progetto della community Fedora che ha l'obiettivo di creare una ampio array di pacchetti per sistemi operativi Linux di livello enterprise. Il progetto ha essenzialmente prodotto pacchetti RHEL e CentOS. AL2 offre un elevato livello di compatibilità con CentOS 7. Di conseguenza, molti pacchetti EPEL7 funzionano su AL2. Tuttavia, AL2023 non supporta i repository EPEL o simili a EPEL.

Uso di cloud-init

In AL2023, cloud-init gestisce il repository dei pacchetti. Per impostazione predefinita, nelle versioni precedenti di Amazon Linux, cloud-init installava gli aggiornamenti di sicurezza. Questa non è l'impostazione predefinita per AL2023. Le nuove funzionalità di aggiornamento deterministico per l'aggiornamento di `releasever` al momento dell'avvio descrivono il modo in cui AL2023 abilita gli aggiornamenti dei pacchetti al momento dell'avvio. Per ulteriori informazioni, consulta Gestione degli aggiornamenti dei pacchetti e del sistema operativo in AL2023 e Aggiornamenti deterministici per la stabilità.

Con AL2023, puoi usare cloud-init con SELinux. Per ulteriori informazioni, consulta Uso di cloud-init per abilitare la modalità `enforcing`.

Cloud-init carica il contenuto della configurazione con cloud-init da posizioni remote utilizzando HTTP(S). Nelle versioni precedenti, Amazon Linux non ti avvisa quando le risorse remote non sono disponibili. In AL2023, le risorse remote non disponibili creano un errore irreversibile e causano la mancata esecuzione di cloud-init. Questa modifica nel comportamento rispetto ad AL2 fornisce un comportamento predefinito di tipo "fail closed" più sicuro.

Per ulteriori informazioni, consulta cloud-init personalizzato e la documentazione di cloud-init.

Supporto per ambiente grafico o desktop

AL2023, incentrato sul cloud e ottimizzato per l'utilizzo di Amazon EC2, attualmente non include un ambiente grafico o desktop. Per fornire un feedback su GitHub, consulta https://github.com/.

Tripletta del compilatore

AL2023 imposta la tripletta del compilatore per GCC e `LLVM` per indicare che il fornitore è `amazon`.

Pertanto, `aarch64-redhat-linux-gcc` AL2 diventa `aarch64-amazon-linux-gcc` su AL2023.

Questo dovrebbe essere completamente trasparente per la maggior parte degli utenti e potrebbe interessare solo coloro che stanno compilando compilatori su AL2023.

Pacchetti x86 (i686) a 32 bit

Come parte della versione 2014.09 di AL1, è stato annunciato che sarebbe stata l'ultima versione a produrre AMI a 32 bit. Pertanto, a partire dal rilascio 2015.03 di AL1, Amazon Linux non supportava più l'esecuzione del sistema in modalità a 32 bit. AL2 offriva un supporto di runtime limitato per i file binari a 32 bit su host x86-64 e non forniva pacchetti di sviluppo per consentire la creazione di nuovi file binari a 32 bit. AL2023 non include più pacchetti di spazio utente a 32 bit. Ti consigliamo 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 di AL2 all'interno di un container AL2 in esecuzione su AL2023.

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

Storicamente, alcuni software richiamavano il comando `lsb_release` (fornito in AL2 dal pacchetto `system-lsb-core`) 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 comando `lsb_release` e non include il pacchetto `system-lsb-core`. Il software deve completare la transizione allo standard `os-release` per mantenere la compatibilità con Amazon Linux e le altre principali distribuzioni Linux.

Modifiche al kernel AL2023 rispetto a AL2

AL2023 include il kernel 6.1 e molte modifiche alla configurazione per ottimizzare ulteriormente Amazon Linux per il cloud. Per la maggior parte degli utenti, queste modifiche dovrebbero essere completamente trasparenti.

Modifiche alla configurazione del kernel incentrate sulla sicurezza

Opzione **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_BUG_ON_DATA_CORRUPTION	n	y	n	y	y	y
CONFIG_DEFAULT_MMAP_MIN_ADDR	4096	4096	4096	4096	65536	65536
CONFIG_DEVMEM	n	y	n	y	n	n
CONFIG_DEVPORT	n	y	n	y	n	n
CONFIG_FORTIFY_SOURCE	n	y	n	y	y	y
CONFIG_HARDENED_USERCOPY_FALLBACK	N/D	N/D	y	y	N/D	N/D
CONFIG_INIT_ON_ALL	N/D	N/D	n	n	n	n

Opzione **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
OC_DEFAULT_ON						
CONFIG_INIT_ON_FREE_DEFAULT_ON	N/D	N/D	n	n	n	n
CONFIG_IOMMU_DEFAULT_DMA_STRICT	N/D	N/D	N/D	N/D	n	n
CONFIG_LDISC_AUTOLOAD	y	y	y	y	n	n
CONFIG_SCHED_CORE	N/D	N/D	N/D	N/D	N/D	y
CONFIG_SCHED_STACK_END_CHECK	n	y	n	y	y	y
CONFIG_SECURITY_DMESG_RESTRICT	n	n	n	n	y	y
CONFIG_SECURITY_SELINUX_DISABLE	y	y	y	y	n	n

Opzione **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SHUFFLE_PAGE_ALLOCATOR	N/D	N/D	y	y	y	y
CONFIG_SLAB_FREELIST_HARDENED	n	y	y	y	y	y
CONFIG_SLAB_FREELIST_RANDOM	n	n	y	y	y	y

Modifiche alla configurazione del kernel incentrate sulla sicurezza specifiche per x86-64

Opzione **CONFIG**	AL2/4.14/x86_64	AL2/5.10/x86_64	AL2023/6.1/x86_64
CONFIG_AMD_IOMMU	y	y	y
CONFIG_AMD_IOMMU_V2	m	m	y
CONFIG_RANDOMIZE_MEMORY	N/D	y	y

Modifiche alla configurazione del kernel incentrate sulla sicurezza specifiche per aarch64 (ARM/Graviton)

Opzione **CONFIG**	AL2/4.14/aarch64	AL2/5.10/aarch64	AL2023/6.1/aarch64
CONFIG_ARM64_PTR_AUTH	N/D	y	y
CONFIG_ARM64_PTR_AUTH_KERNEL	N/D	N/D	y
CONFIG_ARM64_SW_TTBR0_PAN	y	y	y

/dev/mem, **/dev/kmem** e **/dev/port**

Amazon Linux 2023 disabilita `/dev/mem` e `/dev/port` (`CONFIG_DEVMEMeCONFIG_DEVPORT`) completamente, si basa sulle restrizioni già in vigore in AL2.

Il `/dev/kmem` codice è stato completamente rimosso da Linux nel kernel 5.13 e, sebbene fosse disabilitato in AL2, ora non è applicabile ad AL2023.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

FORTIFY_SOURCE

AL2023 è `CONFIG_FORTIFY_SOURCE` abilitato su tutte le architetture supportate. Questa funzionalità mira al rafforzamento della sicurezza. Laddove il compilatore è in grado di determinare e convalidare le dimensioni del buffer, questa funzionalità consente di rilevare gli overflow del buffer nelle funzioni comuni di stringa e memoria.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Caricamento automatico di Line Discipline () **CONFIG_LDISC_AUTOLOAD**

Il kernel AL2023 non caricherà automaticamente le discipline di linea, ad esempio mediante software che utilizza il `TIOCSETDioctl`, a meno che la richiesta non provenga da un processo con i permessi necessari. `CAP_SYS_MODULE`

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

dmesgaccesso per utenti non privilegiati () **CONFIG_SECURITY_DMESG_RESTRICT**

Per impostazione predefinita, AL2023 non consente agli utenti non privilegiati di accedere a. `dmesg`

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Disabilitare SELinux **selinuxfs**

AL2023 disabilita l'opzione obsoleta del `CONFIG_SECURITY_SELINUX_DISABLE` kernel, che abilitava un metodo di runtime per disabilitare SELinux prima del caricamento della policy.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Altre modifiche apportate alla configurazione del kernel

Opzione **CONFIG**	AL2/4.14/ aarch64	AL2/4.14/ x86_64	AL2/5.10/ aarch64	AL2/5.10/ x86_64	AL2023/6. 1/aarch64	AL2023/6. 1/x86_64
CONFIG_HZ	100	250	100	250	100	100
CONFIG_NR_CPUS	4096	8192	4096	8192	512	512
CONFIG_PANIC_ON_OOPS	y	n	y	n	y	y
CONFIG_PANIC_ON_OOPS_VALUE	1	0	1	0	1	1
CONFIG_PPP	m	m	m	m	n	n
CONFIG_SLIP	m	m	m	m	n	n
CONFIG_XEN_PV	N/D	y	N/D	n	N/D	n

CONFIG_HZ

AL2023 è impostato su 100 su entrambe le piattaforme. `CONFIG_HZ` `x86-64` `aarch64`

CONFIG_NR_CPUS

AL2023 imposta `CONFIG_NR_CPUS` un numero più vicino al numero massimo di core CPU presenti in Amazon EC2.

Panic su OOPS

Il kernel AL2023 andrà in panico quando si rompe. Questa funzionalità equivale all'avvio con `oops=panic` dalla riga di comando del kernel.

Un oops del kernel si verifica quando il kernel rileva un errore interno che può influire sull'ulteriore affidabilità del sistema.

Supporto per PPP e SLIP

AL2023 non supporta i protocolli PPP o SLIP.

Supporto per guest Xen PV

AL2023 non supporta l'esecuzione come guest Xen PV.

Supporto per i file system del kernel

Sono state apportate diverse modifiche ai file system che il kernel di AL2 supporterà il montaggio, oltre a cambiamenti negli schemi di partizionamento che il kernel analizzerà.

Opzione **CONFIG**	AL2/4.14/ aarch64	AL2/4.14/ x86_64	AL2/5.10/ aarch64	AL2/5.10/ x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_AFS_FS	n	m	n	m	n	n
CONFIG_AF_RXRPC	n	m	n	m	n	n

Opzione **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_BSD_DISKLABEL	y	y	y	y	n	n
CONFIG_CRAMFS	m	m	m	m	n	n
CONFIG_CRAMFS_BLOCKDEV	N/D	N/D	y	n	N/D	N/D
CONFIG_DM_CLONE	N/D	N/D	n	n	n	n
CONFIG_DM_ERA	m	n	m	n	n	n
CONFIG_DM_INTEGRITY	n	m	n	m	m	m
CONFIG_DM_LOG_WRITES	n	n	m	m	m	m
CONFIG_DM_SWITCH	m	n	m	n	n	n
CONFIG_DM_VERITY	m	n	m	n	n	n
CONFIG_ECRYPT_FS	n	m	n	m	n	n
CONFIG_EXFAT_FS	N/D	N/D	m	m	m	m

Opzione **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_EXT2_FS	n	m	n	m	n	n
CONFIG_EXT3_FS	n	m	n	m	n	n
CONFIG_GFS2_FS	m	m	m	m	n	n
CONFIG_HFSPLUS_FS	n	m	n	m	n	n
CONFIG_HFS_FS	n	m	n	m	n	n
CONFIG_JFS_FS	n	m	n	m	n	n
CONFIG_LDM_PARTITION	n	y	n	y	n	n
CONFIG_MAC_PARTITION	n	y	n	y	n	n
CONFIG_NFS_V2	n	m	n	m	n	n
CONFIG_NTFS_FS	n	m	n	n	n	n
CONFIG_ROMFS_FS	n	m	n	m	n	n

Opzione **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SOLARIS_X86_PARTITION	n	y	n	y	n	n
CONFIG_SQUASHFS_ZSTD	n	y	n	y	y	y
CONFIG_SUN_PARTITION	n	y	n	y	n	n

Supporto per Andrew File System (AFS)

Il kernel non è più compilato con il supporto per il file system `afs`. AL2 non è stato fornito con il supporto dello spazio utente per. `afs`

Supporto per cramfs

Il kernel non è più compilato con il supporto per il file system `cramfs`. Il successore di AL2023 è il file system. `squashfs`

Supporto per BSD disklabel

Il kernel non è più compilato con il supporto per le etichette del disco BSD. Se è necessaria la lettura di volumi con etichette del disco BSD, è possibile avviare più BSD.

Modifiche a Device Mapper

Sono state apportate diverse modifiche ai target Device Mapper configurati nel kernel AL2023.

eCryptFs supporto

Il file system `ecryptfs` è stato dichiarato obsoleto in Amazon Linux. I componenti dello spazio utente di `ecryptfs` erano presenti in AL1, rimossi in AL2 e AL2023 non compila più il kernel con il supporto. `ecryptfs`

exFAT

Il supporto per il `exFAT` file system è stato aggiunto nel kernel 5.10 in AL2. Non era presente al lancio di AL2 con un kernel 4.14. AL2023 continua a supportare il file system. `exFAT`

File system ext2, ext3 e ext4

AL2023 viene fornito con l'`CONFIG_EXT4_USE_FOR_EXT2`opzione, il che significa che il codice del `ext4` file system verrà utilizzato per leggere i `ext2` file system legacy.

CONFIG_GFS2_FS

Il kernel non è più compilato con CONFIG_GFS2_FS.

Supporto per il file system Apple HFS Extended (HFS+)

In AL2, solo i `x86-64` kernel sono stati creati con il supporto del `hfsplus` file system. Il kernel AL2 5.15 non include `hfsplus` il supporto su nessuna architettura. In AL2023, completiamo l'obsolescenza del supporto `hfsplus` in Amazon Linux.

Supporto per il file system HFS

In AL2, solo i `x86-64` kernel sono stati creati con il supporto del file system. `hfs` Il kernel AL2 5.15 non include `hfs` il supporto su nessuna architettura. In AL2023, completiamo l'obsolescenza del supporto `hfs` in Amazon Linux.

Supporto per il file system JFS

In AL2, solo i `x86-64` kernel sono stati creati con il supporto del file system. `jfs` Il kernel AL2 5.15 non include `jfs` il supporto su nessuna architettura. Né AL1 né AL2 sono stati forniti con lo spazio utente JFS. In AL2023, completiamo l'obsolescenza del supporto `jfs` in Amazon Linux.

Il kernel Linux upstream sta valutando la rimozione di. `JFS` Pertanto, se avete dati su un `JFS` file system, dovreste migrarli su un altro file system.

WindowsSupporto per Logical Disk Manager (Dynamic Disk) (**`CONFIG_LDM_PARTITION`**)

AL2023 non supporta più Windows 2000 i Windows XP dischi Windows Vista dinamici con partizioni di MS-DOS stile. Questo codice non ha mai supportato i nuovi dischi dinamici basati su GPT introdotti con. Windows Vista

Supporto per la mappa di partizione Macintosh

AL2023 non supporta più la classica mappa delle partizioni Macintosh. Le versioni recenti di macOS creeranno per impostazione predefinita tabelle di partizione GPT più moderne rispetto a questo tipo precedente.

Supporto per NFSv2

AL2023 non supporta più NFSv2, ma continua a supportare NFSv3, NFSv4, NFSv4.1 e NFSv4.2. Ti consigliamo di migrare a NFSv3 o versioni successive.

NTFS (**`CONFIG_NTFS_FS`**)

Il `ntfs3` codice è stato sostituito `ntfs` per l'accesso ai file system NTFS su Amazon Linux a partire dal kernel 5.10 in AL2. AL2023 non include più il `ntfs` codice e si basa esclusivamente sul codice per accedere ai file system NTFS`ntfs3`.

File system romfs

Il file system `squashfs` è il successore del file system `romfs` in Amazon Linux e il kernel AL2023 non è più compilato con il supporto per `romfs`.

Formato di partizione del disco rigido Solaris x86

AL2023 non supporta più il formato di partizione del disco rigido Solaris x86.

Compressione zstd per **`squashfs`**

AL2023 aggiunge il supporto per i `squashfs` file system zstd compressi su tutte le architetture supportate.

Supporto per tabella di partizione Sun

AL2023 non include più il supporto per il formato della tabella di partizione Sun (). `CONFIG_SUN_PARTITION`

Confronto dei pacchetti installati sulle AMI Amazon Linux 2 e Amazon Linux 2023

Un confronto tra gli RPM presenti sulle AMI standard Amazon Linux 2 e AL2023.

Pacchetto	AMI AL2	AL2023 AMI
GeoIP	1.5.0	
PyYAML	3.10	
acl	2,2,51	2.3.1
acpid	2.0,19	2.0,32
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-extras	2.0.3	
amazon-linux-extras-yum-plugin	2.0.3	
amazon-linux-repo-s3		2023,420240319
amazon-linux-sb-keys		2023,1
amazon-rpm-config		228
amazon-ssm-agent	3,2,2303,0	3,2233,0
at	3,1,13	3,1,23
attr	2,4,46	2.5.1
audit	28,1	30.6
audit-libs	2.8.1	30.6
authconfig	6.2.8	
aws-cfn-bootstrap	2.0	2.0
awscli	1,18,147	

Pacchetto	AMI AL2	AL2023 AMI
awscli-2		2.14.5
basesystem	10,0	11
bash	4,2,46	5,2,15
bash-completion	2.1	2.11
bc	1,006,95	1,07,1
bind-export-libs	9,11,4	
bind-libs	9,11,4	9,16,48
bind-libs-lite	9,11,4	
bind-license	9,11,4	9,16,48
bind-utils	9,11,4	9,16,48
binutils	2,29,1	2,39
blktrace	1.0.5	
boost-date-time	1,53.0 (x86_64)	
boost-filesystem		1.75,0
boost-system	1,53.0 (x86_64)	1.75,0
boost-thread	1,53.0 (x86_64)	1.75,0
bridge-utils	1.5	
bzip2	1.0.6	1.0.8
bzip2-libs	1.0.6	1.0.8
c-ares		1.19.0

Pacchetto	AMI AL2	AL2023 AMI
ca-certificates	2023,2,64	2023,2,64
checkpolicy		3.4
chkconfig	1,7,4	1.15
chrony	4.2	4.3
cloud-init	19,3	222,2
cloud-init-cfg-ec2		222,2
cloud-utils-growpart	0,31	0,31
coreutils	8,22	8,32
coreutils-common		8,32
cpio	2,12	2,13
cracklib	2.9.0	2,9,6
cracklib-dicts	2.9.0	29.6
cronie	1,4,11	
cronie-anacron	1,4,11	
crontabs	1.11	1.11
crypto-policies		20220428
crypto-policies-scripts		20220428
cryptsetup	1,7,4	2.6.1
cryptsetup-libs	17.4	2.6.1
curl	8.3.0	

Pacchetto	AMI AL2	AL2023 AMI
curl-minimal		8,5,0
cyrus-sasl-lib	2,1,26	2,1,27
cyrus-sasl-plain	2,1,26	2,1,27
dbus	1,10,24	1,12,28
dbus-broker		32
dbus-common		1,12,28
dbus-libs	1,10,24	1,12,28
device-mapper	1,02,170	1,02,185
device-mapper-event	1,02,170	
device-mapper-event-libs	1,02,170	
device-mapper-libs	1,02,170	1,02,185
device-mapper-persistent-data	0.7.3	
dhclient	42,5	
dhcp-common	42,5	
dhcp-libs	42,5	
diffutils	3.3	3.8
dmidecode	3.2	
dmraid	1.0.0.rc16	
dmraid-events	1.0.0.rc16	
dnf		4.14.0

Pacchetto	AMI AL2	AL2023 AMI
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugin-support-info		1.2
dnf-plugins-core		4.3.0
dnf-utils		4.3.0
dosfstools	3.0.20	4.2
dracut	033	055
dracut-config-ec2	2.0	3.0
dracut-config-generic	033	055
dwz		0,14
dyninst	9.3.1 (x86_64)	10.2.1
e2fsprogs	1,42,9	1,46,5
e2fsprogs-libs	1,42,9	1,46,5
ec2-hibinit-agent	1.0.8	1.0.8
ec2-instance-connect	1.1	1.1
ec 2- instance-connect-selinux	1.1	1.1
ec2-net-utils	1.7.3	
ec2-utils	1.2	2.2.0
ed	1.9	1.14.2
efi-filesystem		5

Pacchetto	AMI AL2	AL2023 AMI
efi-srpm-macros		5
efibootmgr	15 (ogni arco 64)	
efivar		38
efivar-libs	31 (aarch64)	38
elfutils-debuginfod-client		0.188
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188
elfutils-libs	0,176	0.188
ethtool	4,8	5,15
expat	2.1.0	2.5.0
file	5,11	5,39
file-libs	5,11	5,39
filesystem	3.2	3,14
findutils	4,5,11	4.8.0
fipscheck	1.4.1	
fipscheck-lib	1.4.1	
fonts-srpm-macros		2.0.5
freetype	2.8	
fstrm		0.6.1
fuse-libs	29.2	29.9

Pacchetto	AMI AL2	AL2023 AMI
gawk	40,2	5.1.0
gdbm	1.13	
gdbm-libs		1,19
gdisk	0,8,10	1.0.8
generic-logos	18.0.0	
gettext	0,198,1	0,21
gettext-libs	0,198,1	0,21
ghc-srpm-macros		1.5.0
glib2	2,56,1	2,74,7
glibc	2,26	2,34
glibc-all-langpacks	2,26	2,34
glibc-common	2,26	2,34
glibc-gconv-extra		2,34
glibc-locale-source	2,26	2,34
glibc-minimal-langpack	2,26	
gmp	6.0.0	6.2.1
gnupg2	20,22	
gnupg2-minimal		2.3.7
gnutls		3.8.0
go-srpm-macros		3.2.0

Pacchetto	AMI AL2	AL2023 AMI
gpgme	1.3.2	1.15.1
gpm-libs	1,20,7	1,20.7
grep	2,20	3.8
groff-base	1,22.2	1,22.4
grub2	2,06	
grub2-common	2,06	2,06
grub2-efi-aa64	2,06 (aarch64)	
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)
grub2-efi-aa64-modules	2.06 (nomarzo)	
grub2-efi-x64-ec2	2.06 (x86_64)	2,06 (x86_64)
grub2-pc	2,06 (x86_64)	
grub2-pc-modules	2.06 (nomarzo)	2.06
grub2-tools	2,06	2,06
grub2-tools-minimal	2,06	2,06
grubby	8,28	8,40
gssproxy	0.7.0	0.8.4
gzip	1.5	1.12
hardlink	1.3	
hibagent	1.1.0	
hostname	3.13	3,23

Pacchetto	AMI AL2	AL2023 AMI
hunspell	1.3.2	1.7.0
hunspell-en	0,20121024	0,20140811,1
hunspell-en-GB	0,20121024	0,20140811,1
hunspell-en-US	0,20121024	0,20140811,1
hunspell-filesystem		1.7.0
hwdata	0,252	0,3353
Info	5.1	6.7
inih		49
initscripts	9,49,47	10,09
iproute	5.10.0	5.10.0
iptables	1.8.4	
iptables-libs	1.8.4	
iputils	20180629	20210202
irqbalance	1.7.0	1.9.0
jansson	(2.10)	2.14
jbigkit-libs	2.0	
jitterentropy		3.4.1
jq		1.7.1
json-c	0,11	0,14
kbd	1,15,5	2.4.0

Pacchetto	AMI AL2	AL2023 AMI
kbd-legacy	1,15,5	
kbd-misc	1,15,5	2.4.0
kernel	5,10,210	6,1,79
kernel-livepatch-repo-s3		2023,420240319
kernel-srpm-macros		1
kernel-tools	5,10,210	6,1,79
keyutils	1,5,8	1.6.3
keyutils-libs	1.5.8	1.6.3
kmod	25	29
kmod-libs	25	29
kpartx	0,49	
kpatch-runtime	0.9.4	0,9,7
krb5-libs	1.15.1	1,21
langtable	0,0,31	
langtable-data	0,0,31	
langtable-python	0,0,31	
less	458	608
libacl	2,2,51	2.3.1
libaio	0,3109	0,3111
libarchive		3,5,3

Pacchetto	AMI AL2	AL2023 AMI
libargon2		20171227
libassuan	2.1.0	2,5,5
libattr	2,4,46	2.5.1
libbasicobjects	0,11	01.1
libblkid	2,30,2	2,37,4
libcap	2,54	2,48
libcap-ng	0,7,5	0.8.2
libcbor		0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1,42,9	1,46,5
libcomps		01,20
libconfig	1.4.9	17.2
libcroco	0,6,12	
libcrypt	2,26	
libcurl	8.3,0	
libcurl-minimal		8,5,0
libdaemon	0,14	
libdb	5,3,21	5,3,28
libdb-utils	5,3,21	
libdhash		0,50

Pacchetto	AMI AL2	AL2023 AMI
libdnf		0,69,0
libdrm	2,4,97	
libdwarf	20130207 (x86_64)	
libeconf		0,4,0
libedit	3.0	3.1
libestr	0,19	
libev		4,33
libevent	2.0,21	2,1,12
libfastjson	0,99,4	
libfdisk	2,30,2	2,37,4
libffi	3,0,13	34.4
libfido2		1.10.0
libgcc	7.3.1	11.4.1
libgcrypt	1.5.3	1.10.2
libgomp	7.3.1	11.4.1
libgpg-error	1.12	1,42
libibverbs		48,0
libicu	50,2	
libidn	1,28	
libidn2	2.3.0	2.3.2

Pacchetto	AMI AL2	AL2023 AMI
libini_config	1.3.1	1.3.1
libjpeg-turbo	2.0,90	
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libldb		26.2
libmaxminddb		1.5.2
libmetalink	0,13	0,13
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2,30,2	2,37,4
libnetfilter_conntrack	1.0.6	
libnfnetlink	1.0.1	
libnfsidmap	0.25	2,5,4
libnghttp2	1,41,0	1,57,0
libnl3	3,2,28	3.5.0
libnl3-cli	3,2,28	
libpath_utils	0,21	0,2,1
libpcap	1.5.3	1.10.1
libpciaccess	0,14 (x86_64)	
libpipeline	1.2.3	1.5.3

Pacchetto	AMI AL2	AL2023 AMI
libpkgconf		1.8.0
libpng	1.5.13	
libpsl	0,21,5	0,21,1
libpwquality	1.2.3	1.4.4
libref_array	0,1,5	0,1,5
librepo		1,14,5
libreport-filesystem		2,15,2
libseccomp	2.5.2	2.5.3
libselinux	2.5	3.4
libselinux-utils	2.5	3.4
libsemanage	2.5	3.4
libsepol	2.5	3.4
libsigsegv		2,13
libsmartcols	2,30,2	2,37,4
libsolv		0,7,22
libss	1,42,9	1,46,5
libssh2	1.4.3	
libsss_certmap		2,9,4
libsss_idmap	1,16,5	2,9,4
libsss_nss_idmap	1,16,5	2,9,4

Pacchetto	AMI AL2	AL2023 AMI
libsss_sudo		2.9.4
libstdc++	7.3.1	11.4.1
libstoragemgmt	1.6.1	1.9.4
libstoragemgmt-python	1.6.1	
libstoragemgmt-python-clibs	1.6.1	
libsysfs	2.1.0	
libtalloc		2.3.4
libtasn1	4,10	4,19,0
libtdb		1.4.7
libteam	1,27	
libtevent		0.13.0
libtextstyle		0,21
libtiff	40,3	
libtirpc	0,2,4	1.3.3
libunistring	0,9,3	0,9,10
libuser	0,60	0,63
libutempter	1.1.6	1.2.1
libuuid	2,30,2	2,37,4
libuv		1.47.0
libverto	02,5	0,32

Pacchetto	AMI AL2	AL2023 AMI
libverto-libev		0,32
libverto-libevent	02,5	
libwebp	0,3,0	
libxcrypt		4,4,33
libxml2	2,9,1	210.4
libxml2-python	29.1	
libyaml	0,14	02,5
libzstd		1,5,5
lm_sensors-libs	3.4.0	3.6.0
lmdb-libs		0,9,29
logrotate	3,86	3,20,1
lsof	4,87	4,94,0
lua	5.1.4	
lua-libs		5.4.4
lua-srpm-macros		1
lvm2	2,02,187	
lvm2-libs	2,02,187	
lz4	1,7,5	
lz4-libs		1.9.4
make	3,82	

Pacchetto	AMI AL2	AL2023 AMI
man-db	26.3	29.3
man-pages	3,53	5,10
man-pages-overrides	7,5,2	
mariadb-libs	5,5,68	
mdadm	4.0	
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)
mlocate	0,26	
mpfr		4.1.0
mtr	0.92	
nano	2,9,8	5.8
ncurses	6.0	6.2
ncurses-base	6.0	6.2
ncurses-libs	6.0	6.2
net-tools	2.0	2.0
nettle	2.7.1	3.8
newt	0,52,15	0,52,21
newt-python	0,52,15	
nfs-utils	1.3.0	2,5,4
npth		1.6
nspr	4,35,0	4,35,0

Pacchetto	AMI AL2	AL2023 AMI
nss	3,90,0	3,90,0
nss-pem	1.0.3	
nss-softokn	3,90,0	3,90,0
nss-softokn-freebl	3,90,0	3,90,0
nss-sysinit	3,90,0	3,90,0
nss-tools	3,90,0	
nss-util	3,90,0	3,90,0
ntsysv	17.4	1.15
numactl-libs	2.0.9	2.0,14
ocaml-srpm-macros		6
oniguruma		6,9,7,1
openblas-srpm-macros		2
openldap	2,4,44	2,4,57
openssh	7,4p 1	8,7p1
openssh-clients	7,4p1	8,7p1
openssh-server	7,4p1	8,7p1
openssl	1,0,2k	3,0,8
openssl-libs	1,0,2k	3,0,8
openssl-pkcs11		0,4,12
os-prober	1.58	1,77

Pacchetto	AMI AL2	AL2023 AMI
p11-kit	0,23,22	0,24,1
p11-kit-trust	0,23,22	0,24,1
package-notes-srpm-macros		0.4
pam	1.1.8	1.5.1
parted	3.1	3.4
passwd	0,79	0,80
pciutils	35,1	3.7.0
pciutils-libs	35.1	3.7.0
pcre	8,32	
pcre2	10,23	10,40
pcre2-syntax		10,40
perl	5,16,3	
perl-Carp	1,26	1,50
perl-Class-Struct		0,66
perl- DynaLoader		1,47
perl-Encode	2,51	3,15
perl-Errno		1,30
perl-Exporter	5,68	5,74
perl-Fcntl		1.13
perl-File-Basename		2,85

Pacchetto	AMI AL2	AL2023 AMI
perl-File-Path	2,09	2,18
perl-File-Temp	0,23,01	0,231,100
perl-File-stat		1,09
perl-Filter	1,49	
perl-Getopt-Long	2,40	2,52
perl-Getopt-Std		1.12
perl-HTTP-Tiny	0,033	0,078
perl-IO		1,43
perl-IPC-Open3		1,21
perl-MIME-Base64		3,16
perl-POSIX		1,94
perl- PathTools	3,40	3,78
perl-Pod-Escapes	1.04	1,07
perl-Pod-Perldoc	3,20	3,28,01
perl-Pod-Simple	3,28	3,42
perl-Pod-Usage	1,63	2,01
perl-Scalar-List-Utils	1,27	1,56
perl- SelectSaver		1.02
perl-Socket	2.010	2,032
perl-Storable	2,45	3,21

Pacchetto	AMI AL2	AL2023 AMI
perl-Symbol		1,08
perl-Term-ANSIColor		5,01
perl-Term-Cap		1,17
Testo in Perl- ParseWords	3.29	3,30
perl-Text-Tabs+Wrap		2021,0726
Tempo Perl- HiRes	1,9725	
perl-Time-Local	1,2300	1.300
perl-constant	1,27	1,33
perl-if		0,60,800
perl-interpreter		5,32,1
perl-libs	5,16,3	5,32,1
perl-macros	5,16,3	
perl-mro		1,23
perl-overload		1,31
perl-overloading		0,02
perl-parent	0,225	0,238
perl-podlators	2.5.1	4,14
perl-srpm-macros		1
perl-subs		1,03
perl-threads	1,87	

Pacchetto	AMI AL2	AL2023 AMI
perl-threads-shared	1,43	
perl-vars		1,05
pinentry	0.8.1	
pkgconf		1.8.0
pkgconf-m4		1.8.0
pkgconf-pkg-config		1.8.0
pkgconfig	0,27,1	
plymouth	0,89	
plymouth-core-libs	0,89	
plymouth-scripts	0,89	
pm-utils	1.4.1	
policycoreutils	2.5	3.4
policycoreutils-python-utils		3.4
popt	1.13	1,18
postfix	210.1	
procps-ng	3,3,10	3,3,17
protobuf-c		1.4.1
psacct	6.6.1	6.6.4
psmisc	22,20	23,4
pth	2.0.7	

Pacchetto	AMI AL2	AL2023 AMI
publicsuffix-list-dafsa	20240208	20240212
pygpgme	0.3	
pyliblzma	0,53	
pystache	0,5,3	
python	2,7,18	
python-babel	0.9.6	
python-backports	1	
python-backports-ssl_match_hostname	3.5.0.1	
python-cffi	1.6.0	
python-chardet	2.2.1	
python-chevron		0.13.1
python-configobj	4,7,2	
python-daemon	1.6	
python-devel	2,7,18	
python-docutils	0,12	
python-enum34	1.0.4	
python-idna	2.4	
python-iniparse	0.4	
python-ipaddress	1,0,16	
python-jinja2	2,7,2	

Pacchetto	AMI AL2	AL2023 AMI
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	
python-pycurl	7,19,0	
python-repoze-lru	0.4	
python-requests	2.6.0	
python-simplejson	3.2.0	
python-srpm-macros		3.9
python-urlgrabber	3,10	
python-urllib3	1,25,9	
python2-botocore	1.18,6	
python2-colorama	0,39	
python2-cryptography	17.2	

Pacchetto	AMI AL2	AL2023 AMI
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	
python3	3,7,16	3,9,16
python3-attrs		20,3,0
python3-audit		30.6
python3-awscrt		0,19,19
python3-babel		2,9,1
python3-cffi		1,14,5
python3-chardet		4.0.0
python3-colorama		04.4
python3-configobj		50.6

Pacchetto	AMI AL2	AL2023 AMI
python3-cryptography		36,0
python3-daemon	2.2.3	2.3.0
python3-dateutil		28.1
python3-dbus		1,2,18
python3-distro		1.5.0
python3-dnf		4.14.0
python 3- dnf-plugins-core		4.3.0
python3-docutils	0,14	0,16
python3-gpg		1.15.1
python3-hawkey		0,69,0
python3-idna		(2.10)
python3-jinja2		211,3
python3-jmespath		0.10.0
python3-jsonpatch		1,21
python3-jsonpointer		2.0
python3-jsonschema		3.2.0
python3-libcomps		01,20
python3-libdnf		0,69,0
python3-libs	3,7,16	3,9,16
python3-libselinux		3.4

Pacchetto	AMI AL2	AL2023 AMI
python3-libsemanage		3.4
python3-libstoragemgmt		1.9.4
python3-lockfile	0.11.0	0.12.2
python3-markupsafe		1.1.1
python3-netifaces		0,10,6
python3-oauthlib		3.0.2
python3-pip	202,2	
python3-pip-wheel		21,31
python3-ply		3,11
python3-policycoreutils		3.4
python3-prettytable		0.7.2
python3-prompt-toolkit		3,0,24
python3-pycparser		2,20
python3-pyrsistent		0,17,3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pystache	0,5,4	
python3-pytz		2022,7,1
python3-pyyaml		5.4.1
python3-requests		2,25,1

Pacchetto	AMI AL2	AL2023 AMI
python3-rpm		4,161,3
python3-ruamel-yaml		0,16,6
pitone 3- ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools	49,13	59,60
python3-setuptools-wheel		59,6,0
python3-simplejson	3.2.0	
python3-six		1.15.0
sistema python3		235
python3-urllib3		1,25,10
python3-wcwidth		0,2,5
pyxattr	0,5,1	
qrencode-libs	3.4.1	
quota	4,01	4,06
quota-nls	4,01	4,06
rdate	1.4	
readline	6.2	8.1
rng-tools	6.8	6,14
rootfiles	8.1	8.1
rpcbind	0,2,0	1.2.6

Pacchetto	AMI AL2	AL2023 AMI
rpm	4.11.3	4,161,3
rpm-build-libs	4.11,3	4,161,3
rpm-libs	4.11,3	4,161,3
rpm-plugin-selinux		4,161,3
rpm-plugin-systemd-inhibit	4.11,3	4,161,3
rpm-sign-libs		4,161,3
rsync	3.1.2	3.2.6
rsyslog	8,24,0	
rust-srpm-macros		21
sbsigntools		0.9.4
scl-utils	20130529	
screen	4.1.0	4.8.0
sed	42,2	4.8
selinux-policy	3,13,1	37,22
selinux-policy-targeted	3,13,1	37,22
setserial	2,17	
setup	2,8,71	2,13,7
setuptool	1,19,11	
sgpio	1,2,0,10	
shadow-utils	4.1.5.1	4.9

Pacchetto	AMI AL2	AL2023 AMI
shared-mime-info	1.8	
slang	2.2.4	2.3.2
sqlite	3,7,17	
sqlite-libs		3,4,0
sssd-client	1,16,5	2,9,4
sssd-common		2,9,4
sssd-kcm		2,9,4
sssd-nfs-idmap		2,9,4
strace	4,26	5,16
sudo	1,8,23	1,9,14
sysctl-defaults	1.0	1
sysstat	101,5	12,5,6
system-release	2	2023,420240319
systemd	219	252,16
systemd-libs	219	252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-sysv	219	
systemd-udev		252,16

Pacchetto	AMI AL2	AL2023 AMI
systemtap-runtime	4,5	4.8
sysvinit-tools	2,88	
tar	1,26	1,34
tbb		2020,3
tcp_wrappers	7.6	
tcp_wrappers-libs	7.6	
tcpdump	4,9,2	4,99,1
tcsh	6,18,01	6,24,07
teamd	1,27	
time	1,7	1.9
traceroute	20,22	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	1.1.2	2.2
usermode	1,111	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2,30,2	2,37,4
util-linux-core		2,37,4
vim-common	9,0,2153	9,0,2153

Pacchetto	AMI AL2	AL2023 AMI
vim-data	9,0,2153	9,0,2153
vim-enhanced	9,0,2153	9,0,2153
vim-filesystem	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153
virt-what	1,18	
wget	1.14	1,21,3
which	2,20	2,21
words	3.0	3.0
xfsdump	3,18	3,1,11
xfsprogs	5.0.0	5,18,0
xxd	9,0,2153	9,0,2153
xxhash-libs		0.8.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yajl	2.0.4	
yum	3.4.3	4.14.0
yum-langpacks	04.2	
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1,1,31	
yum-utils	1,1,31	

Pacchetto	AMI AL2	AL2023 AMI
zip	3.0	3.0
zlib	1.2.7	1,2,11
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1,5,5

Confronto dei pacchetti installati sulle AMI minime Amazon Linux 2 e Amazon Linux 2023

Un confronto tra gli RPM presenti sulle AMI minimali Amazon Linux 2 e AL2023.

Pacchetto	AL2 Minimal	AL2023 Minimo
PyYAML	3.10	
acl	2,2,51	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-extras	2.0.3	
amazon-linux-repo-s3		2023,420240319
amazon-linux-sb-keys		2023,1
audit	28,1	30.6
audit-libs	2.8.1	30.6

Pacchetto	AL2 Minimal	AL2023 Minimo
authconfig	6.2.8	
awscli-2		2.14.5
basesystem	10,0	11
bash	4,2,46	5,2,15
bind-export-libs	9,11,4	
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,64	2023,2,64
checkpolicy		3.4
chkconfig	1,7,4	
chrony	4.2	4.3
cloud-init	19,3	222,2
cloud-init-cfg-ec2		222,2
cloud-utils-growpart	0,31	0,31
coreutils	8,22	8,32
coreutils-common		8,32
cpio	2,12	2,13
cracklib	2.9.0	2,9,6
cracklib-dicts	2.9.0	29.6
cronie	1,4,11	
cronie-anacron	1,4,11	

Pacchetto	AL2 Minimal	AL2023 Minimo
crontabs	1.11	
crypto-policies		20220428
cryptsetup-libs	1,7,4	2.6.1
curl	8.3.0	
curl-minimal		8,5,0
cyrus-sasl-lib	2,1,26	2,1,27
dbus	1,10,24	1,12,28
dbus-broker		32
dbus-common		1,12,28
dbus-libs	1,10,24	1,12,28
device-mapper	1,02,170	1,02,185
device-mapper-libs	1,02,170	1,02,185
dhclient	42,5	
dhcp-common	42,5	
dhcp-libs	42,5	
diffutils	3.3	3.8
dnf		4.14.0
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugin-support-info		1.2

Pacchetto	AL2 Minimal	AL2023 Minimo
dnf-plugins-core		4.3.0
dracut	033	055
dracut-config-ec2	2.0	3.0
dracut-config-generic	033	055
e2fsprogs	1,42,9	1,46,5
e2fsprogs-libs	1,42,9	1,46,5
ec2-utils	1.2	2.2.0
efi-filesystem		5
efibootmgr	15 (ogni arco 64)	
efivar		38
efivar-libs	31 (aarch64)	38
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188
elfutils-libs	0,176	0.188
expat	2.1.0	2.5.0
file	5,11	5,39
file-libs	5,11	5,39
filesystem	3.2	3,14
findutils	4,5,11	4.8.0
fipscheck	1.4.1	

Pacchetto	AL2 Minimal	AL2023 Minimo
fipscheck-lib	1.4.1	
freetype	2.8	
fuse-libs	29.2	29.9
gawk	40,2	5.1.0
gdbm	1.13	
gdbm-libs		1,19
gdisk	0,8,10	1.0.8
gettext	0,198,1	0,21
gettext-libs	0,198,1	0,21
glib2	2,56,1	2,74,7
glibc	2,26	2,34
glibc-all-langpacks	2,26	2,34
glibc-common	2,26	2,34
glibc-locale-source	2,26	2,34
glibc-minimal-langpack	2,26	
gmp	6.0.0	6.2.1
gnupg2	20,22	
gnupg2-minimal		2.3.7
gnutls		3.8.0
gpgme	1.3.2	1.15.1

Pacchetto	AL2 Minimal	AL2023 Minimo
grep	2,20	3.8
groff-base	1,22.2	1,22.4
grub2	2,06	
grub2-common	2,06	2,06
grub2-efi-aa64	2,06 (aarch64)	
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)
grub2-efi-aa64-modules	2.06 (nomarzo)	
grub2-efi-x64-ec2	2.06 (x86_64)	2,06 (x86_64)
grub2-pc	2,06 (x86_64)	
grub2-pc-modules	2.06 (nomarzo)	2.06
grub2-tools	2,06	2,06
grub2-tools-minimal	2,06	2,06
grubby	8,28	8,40
gzip	1.5	1.12
hardlink	1.3	
hostname	3.13	3,23
hwdata		0,3353
Info	5.1	
inih		49
initscripts	9,49,47	10,09

Pacchetto	AL2 Minimal	AL2023 Minimo
iproute	5.10.0	5.10.0
iptables	1.8.4	
iptables-libs	1.8.4	
iputils	20180629	20210202
irqbalance	1.7.0	1.9.0
jansson		2.14
jitterentropy		3.4.1
jq		1.7.1
json-c		0,14
kbd		2.4.0
kbd-misc		2.4.0
kernel	4,148336	6,1,79
kernel-livepatch-repo-s3		2023,420240319
keyutils-libs	1,5,8	1.6.3
kmod	25	29
kmod-libs	25	29
kpartx	0,49	
krb5-libs	1.15.1	1,21
less	458	608
libacl	2,2,51	2.3.1

Pacchetto	AL2 Minimal	AL2023 Minimo
libarchive		3,5,3
libargon2		20171227
libassuan	2.1.0	2,5,5
libattr	2,4,46	2.5.1
libblkid	2,30,2	2,37,4
libcap	2,54	2,48
libcap-ng	0,7,5	0.8.2
libcbor		0.7.0
libcom_err	1,42,9	1,46,5
libcomps		01,20
libcroco	0,6,12	
libcrypt	2,26	
libcurl	8.3,0	
libcurl-minimal		8,5,0
libdb	5,3,21	5,3,28
libdb-utils	5,3,21	
libdnf		0,69,0
libeconf		0,40
libedit	3.0	3.1
libestr	0,19	

Pacchetto	AL2 Minimal	AL2023 Minimo
libfastjson	0,99,4	
libfdisk	2,30,2	2,37,4
libffi	3,0,13	34.4
libfido2		1.10.0
libgcc	7.3.1	11.4.1
libgcrypt	1.5.3	1.10.2
libgomp	7.3.1	11.4.1
libgpg-error	1.12	1,42
libicu	50,2	
libidn	1,28	
libidn2	2.3.0	2.3.2
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libmetalink	0,13	
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2,30,2	2,37,4
libnetfilter_conntrack	1.0.6	
libnfnetlink	1.0.1	
libnghttp2	1,41,0	1,57,0

Pacchetto	AL2 Minimal	AL2023 Minimo
libpcap	1.5.3	
libpipeline	1.2.3	1.5.3
libpng	1,5,13	
libpsl	0,21,5	0,21,1
libpwquality	1.2.3	1.4.4
librepo		1,14,5
libreport-filesystem		2,15,2
libseccomp	2.5.2	2.5.3
libselinux	2.5	3.4
libselinux-utils	2.5	3.4
libsemanage	2.5	3.4
libsepol	2.5	3.4
libsigsegv		2,13
libsmartcols	2,30,2	2,37,4
libsolv		0,7,22
libss	1,42,9	1,46,5
libssh2	1.4.3	
libstdc++	7.3.1	11.4.1
libsysfs	2.1.0	
libtasn1	4,10	4,19,0

Pacchetto	AL2 Minimal	AL2023 Minimo
libtextstyle		0,21
libunistring	0,9,3	0,9,10
libuser	0,60	0,63
libutempter	1.1.6	1.2.1
libuuid	2,30,2	2,37,4
libverto	02,5	0,32
libxcrypt		4,4,33
libxml2	2,9,1	210.4
libyaml	0,14	02,5
libzstd		1,5,5
logrotate	38.6	3,20,1
lua	5.1.4	
lua-libs		5.4.4
lz4	1,7,5	
lz4-libs		1.9.4
make	3,82	
man-db	26.3	29.3
mariadb-libs	5,5,68	
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)
mpfr		4.1.0

Pacchetto	AL2 Minimal	AL2023 Minimo
ncurses	6.0	6.2
ncurses-base	6.0	6.2
ncurses-libs	6.0	6.2
net-tools	2.0	2.0
nettle	2.7.1	3.8
newt	0,52,15	
newt-python	0,52,15	
npth		1.6
nspr	4,35,0	
nss	3,90,0	
nss-pem	1.0.3	
nss-softokn	3,90,0	
nss-softokn-freebl	3,90,0	
nss-sysinit	3,90,0	
nss-tools	3,90,0	
nss-util	3,90,0	
numactl-libs	20,9	2.0,14
oniguruma		6,9,7,1
openldap	2,4,44	2,4,57
openssh	7,4p 1	8,7p1

Pacchetto	AL2 Minimal	AL2023 Minimo
openssh-clients	7,4p1	8,7p1
openssh-server	7,4p1	8,7p1
openssl	1,0,2k	3,0,8
openssl-libs	1,0,2k	3,0,8
openssl-pkcs11		0,4,12
os-prober	1.58	1,77
p11-kit	0,23,22	0,24,1
p11-kit-trust	0,23,22	0,24,1
pam	1.1.8	1.5.1
passwd	0,79	0,80
pciutils		3.7.0
pciutils-libs		3.7.0
pcre	8,32	
pcre2	10,23	10,40
pcre2-syntax		10,40
pinentry	0.8.1	
pkgconfig	0,27,1	
policycoreutils	2.5	3.4
popt	1.13	1,18
postfix	210.1	

Pacchetto	AL2 Minimal	AL2023 Minimo
procps-ng	3,3,10	3,3,17
psmisc	22,20	23,4
pth	2.0.7	
publicsuffix-list-dafsa	20240208	20240212
pygpgme	0.3	
pyliblzma	0,53	
python	2,7,18	
python-babel	0.9.6	
python-backports	1	
python-backports-ssl_match_hostname	3.5.0.1	
python-cffi	1.6.0	
python-chardet	2.2.1	
python-configobj	4,7,2	
python-devel	2,7,18	
python-enum34	1.0.4	
python-idna	2.4	
python-iniparse	0.4	
python-ipaddress	1,0,16	
python-jinja2	2,7,2	
python-jsonpatch	1.2	

Pacchetto	AL2 Minimal	AL2023 Minimo
python-jsonpointer	1.9	
python-jwcrypto	0,4,2	
python-libs	2,7,18	
python-markupsafe	0,11	
python-ply	3.4	
python-pycparser	2.14	
python-pycurl	7,19,0	
python-repoze-lru	0.4	
python-requests	2.6.0	
python-urlgrabber	3,10	
python-urllib3	1,25,9	
python2-cryptography	1.7.2	
python2-jsonschema	2.5.1	
python2-oauthlib	2.0.1	
python2-pyasn1	0,19	
python2-rpm	4.11.3	
python2-setuptools	41,2,0	
python2-six	1.11.0	
python3		3,9,16
python3-attrs		20,3,0

Pacchetto	AL2 Minimal	AL2023 Minimo
python3-audit		30.6
python3-awscrt		0,19,19
python3-babel		2,9,1
python3-cffi		1,14,5
python3-chardet		4.0.0
python3-colorama		04.4
python3-configobj		5.0.6
python3-cryptography		36,0
python3-dateutil		28.1
python3-dbus		1,2,18
python3-distro		1.5.0
python3-dnf		4.14.0
python 3- dnf-plugins-core		4.3.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0,69,0
python3-idna		(2.10)
python3-jinja2		211,3
python3-jmespath		0.10.0
python3-jsonpatch		1,21

Pacchetto	AL2 Minimal	AL2023 Minimo
python3-jsonpointer		2.0
python3-jsonschema		3.2.0
python3-libcomps		01,20
python3-libdnf		0,69,0
python3-libs		3,9,16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-markupsafe		1.1.1
python3-netifaces		0,10,6
python3-oauthlib		3.0.2
python3-pip-wheel		21,31
python3-ply		3,11
python3-policycoreutils		3.4
python3-prettytable		0.7.2
python3-prompt-toolkit		3,0,24
python3-pycparser		2,20
python3-pyrsistent		0,17,3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022,7,1

Pacchetto	AL2 Minimal	AL2023 Minimo
python3-pyyaml		5.4.1
python3-requests		2,25,1
python3-rpm		4,161,3
python3-ruamel-yaml		0,16,6
pitone 3- ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59,60
python3-setuptools-wheel		59,6,0
python3-six		1.15.0
sistema python3		235
python3-urllib3		1,25,10
python3-wcwidth		0,2,5
pyxattr	0,5,1	
qrencode-libs	3.4.1	
readline	6.2	8.1
rng-tools	6.8	6,14
rootfiles	8.1	8.1
rpm	4.11.3	4,161,3
rpm-build-libs	411,3	4,161,3
rpm-libs	411,3	4,161,3

Pacchetto	AL2 Minimal	AL2023 Minimo
rpm-plugin-selinux		4,161,3
rpm-plugin-systemd-inhibit	411,3	4,161,3
rpm-sign-libs		4,161,3
rsyslog	8,24,0	
sbsigntools		0.9.4
sed	4.2.2	4.8
selinux-policy	3,13,1	37,22
selinux-policy-targeted	3,13,1	37,22
setup	2,8,71	2,13,7
shadow-utils	4.1.5.1	4.9
shared-mime-info	1.8	
slang	2.2.4	
sqlite	3,7,17	
sqlite-libs		3,4,0
sudo	1,8,23	1,9,14
sysctl-defaults	1.0	1
system-release	2	2023,420240319
systemd	219	252,16
systemd-libs	219	252,16
systemd-networkd		252,16

Pacchetto	AL2 Minimal	AL2023 Minimo
systemd-pam		252,16
systemd-resolved		252,16
systemd-sysv	219	
systemd-udev		252,16
sysvinit-tools	2,88	
tar	1,26	1,34
tcp_wrappers-libs	7.6	
tzdata	2024a	2024a
update-motd	1.1.2	2.2
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2,30,2	2,37,4
util-linux-core		2,37,4
vim-data	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153
which	2,20	2,21
xfsprogs	5.0.0	5,18,0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0

Pacchetto	AL2 Minimal	AL2023 Minimo
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1,1,31	
zlib	1.2.7	1,2,11
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1,5,5

Confronto dei pacchetti installati sulle immagini dei container di base Amazon Linux 2 e Amazon Linux 2023

Un confronto tra gli RPM presenti nelle immagini dei container di base Amazon Linux 2 e AL2023.

Pacchetto	Contenitore AL2	Contenitore AL2023
alternatives		1.15
amazon-linux-extras	2.0.3	
amazon-linux-repo-cdn		2023,420240319
audit-libs		3,0,6
basesystem	10,0	11
bash	4,2,46	5,2,15
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,64	2023,2,64
chkconfig	1,7,4	

Pacchetto	Contenitore AL2	Contenitore AL2023
coreutils	8,22	
coreutils-single		8,32
cpio	2,12	
crypto-policies		20220428
curl	8,3,0	
curl-minimal		8,5,0
cyrus-sasl-lib	2,1,26	
diffutils	3.3	
dnf		4.14.0
dnf-data		4.14.0
elfutils-default-yama-scope		0.188
elfutils-libelf	0,176	0.188
elfutils-libs		0.188
expat	2.1.0	2.5.0
file-libs	5,11	5,39
filesystem	3.2	3,14
findutils	4,5,11	
gawk	40,2	5.1.0
gdbm	1.13	
gdbm-libs		1,19

Pacchetto	Contenitore AL2	Contenitore AL2023
glib2	2,56,1	2,74,7
glibc	2,26	2,34
glibc-common	2,26	2,34
glibc-langpack-en	2,26	
glibc-minimal-langpack	2,26	2,34
gmp	6.0.0	62,1
gnupg2	20,22	
gnupg2-minimal		2.3.7
gpgme	1.3.2	1.15.1
grep	2,20	3.8
Info	5.1	
json-c		0,14
keyutils-libs	1.5.8	1.6.3
krb5-libs	1.15.1	1,21
libacl	2,2,51	2.3.1
libarchive		3,5,3
libassuan	2.1.0	2,5,5
libattr	2,4,46	2.5.1
libblkid	2,30,2	2,37,4
libcap	2,54	2,48

Pacchetto	Contenitore AL2	Contenitore AL2023
libcap-ng		0.8.2
libcom_err	1,42,9	1,46,5
libcomps		01,20
libcrypt	2,26	
libcurl	8.3,0	
libcurl-minimal		8,5,0
libdb	5,3,21	
libdb-utils	5,3,21	
libdnf		0,69,0
libffi	3,0,13	34.4
libgcc	7.3.1	114,1
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.12	1,42
libidn2	2.3.0	2.3.2
libmetalink	0,13	
libmodulemd		2.13.0
libmount	2,30,2	2,37,4
libnghttp2	1,41,0	1,57,0
libpsl	0,21,5	0,21,1

Pacchetto	Contenitore AL2	Contenitore AL2023
librepo		1,14,5
libreport-filesystem		2,15,2
libselinux	2.5	3.4
libsepol	2.5	3.4
libsigsegv		2,13
libsmartcols		2,37,4
libsolv		0,7,22
libssh2	1.4.3	
libstdc++	7.3.1	11,4,1
libtasn1	4,10	4,19,0
libunistring	0,9,3	0,9,10
libuuid	2,30,2	2,37,4
libverto	0,2,5	0,32
libxcrypt		4,4,33
libxml2	2,9,1	210.4
libyaml		02,5
libzstd		1,5,5
lua	5.1.4	
lua-libs		5.4.4
lz4-libs		1.9.4

Pacchetto	Contenitore AL2	Contenitore AL2023
mpfr		4.1.0
ncurses	6.0	
ncurses-base	6.0	6.2
ncurses-libs	6.0	6.2
npth		1.6
nspr	4,35,0	
nss	3,90,0	
nss-pem	1.0.3	
nss-softokn	3,90,0	
nss-softokn-freebl	3,90,0	
nss-sysinit	3,90,0	
nss-tools	3,90,0	
nss-util	3,90,0	
openldap	2,4,44	
openssl-libs	1,0,2k	3,0,8
p11-kit	0,23,22	0,24,1
p11-kit-trust	0,23,22	0,24,1
pcre	8,32	
pcre2		10,40
pcre2-syntax		10,40

Pacchetto	Contenitore AL2	Contenitore AL2023
pinentry	0.8.1	
popt	1.13	1,18
pth	2.0.7	
publicsuffix-list-dafsa	20240208	20240212
pygpgme	0.3	
pyliblzma	0,53	
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	
python3		3,9,16
python3-dnf		4.14.0
python3-gpg		1.15.1
python3-hawkey		0,69,0
python3-libcomps		01,20
python3-libdnf		0,69,0
python3-libs		3,9,16
python3-pip-wheel		21,31

Pacchetto	Contenitore AL2	Contenitore AL2023
python3-rpm		4,161,3
python3-setuptools-wheel		59,60
pyxattr	0,5,1	
readline	6.2	8.1
rpm	4.11.3	4,161,3
rpm-build-libs	411,3	4,161,3
rpm-libs	411,3	4,161,3
rpm-sign-libs		4,161,3
sed	4.2.2	4.8
setup	2,8,71	2,13,7
shared-mime-info	1.8	
sqlite	3,7,17	
sqlite-libs		3,4,0
system-release	2	2023,420240319
tzdata	2024a	2024a
vim-data	9,0,2153	
vim-minimal	9,0,2153	
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	

Pacchetto	Contenitore AL2	Contenitore AL2023
yum-plugin-ovl	1,1,31	
yum-plugin-priorities	1,1,31	
zlib	1.2.7	1,2,11

Confronto tra AL1 e AL2023

I seguenti argomenti descrivono le differenze chiave tra AL1 e AL2023 che non sono già state trattate dal confronto con AL2.

> **Note**
>
> AL1 ha raggiunto il suo end-of-life (EOL) il 31 dicembre 2023 e non riceverà aggiornamenti di sicurezza o correzioni di bug a partire dal 1° gennaio 2024. Per ulteriori informazioni su AL1 EOL e sul supporto di manutenzione, consulta il post del blog Update on Amazon Linux AMI. end-of-life Ti consigliamo di aggiornare le applicazioni ad AL2023, che include il supporto a lungo termine fino al 2028.

Argomenti

Supporto per ogni rilascio

Per AL2023, offriamo cinque anni di supporto dalla data di rilascio. AL1 ha terminato il supporto standard il 31 dicembre 2020 e il supporto di manutenzione il 31 dicembre 2023.

Per ulteriori informazioni, consulta Cadenza di rilascio.

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

In AL2 `upstart` è stato sostituito da `systemd` as the `init` system. AL2023 utilizza anche `systemd` come `init` sistema, adottando ulteriormente nuove caratteristiche e funzionalità di. `systemd`

Python 2.6 e 2.7 sono stati sostituti con Python 3

Sebbene AL1 abbia contrassegnato Python 2.6 come EOL nella versione 2018.03, i pacchetti erano ancora disponibili nei repository per l'installazione. AL2 è stato fornito con Python 2.7 come prima versione Python supportata e AL2023 completa la transizione a Python 3. Nessuna versione di Python 2.x è inclusa nei repository AL2023.

Per ulteriori informazioni su Python su Amazon Linux, consulta Python in AL2023.

OpenJDK 8 come JDK più vecchio

AL2023 viene fornito con Amazon Corretto come Java Development Kit (JDK) predefinito (e unico). Tutti i pacchetti Java basati in AL2023 sono compilati con. Amazon Corretto 17

In AL1, OpenJDK 1.6.0 `java-1.6.0-openjdk` () è diventato EOL con la prima versione 2018.03 e OpenJDK 1.7.0 () è diventato EOL a metà 2020, sebbene entrambe le versioni fossero disponibili nei repository `java-1.7.0-openjdk` AL1. La prima versione di OpenJDK disponibile in AL2023 è OpenJDK 8, fornita da. Amazon Corretto 8

Modifiche al kernel AL2023 rispetto ad Amazon Linux 1 (AL1)

Applicazione di patch live del kernel

Sia AL2023 che AL2 aggiungono il supporto per la funzionalità di live-patching del kernel. Ciò consente di correggere vulnerabilità di sicurezza critiche e importanti nel kernel Linux senza riavvio o tempi di inattività. Per ulteriori informazioni, consulta Applicazione di patch Kernel Live su AL2023.

Supporto del file system del kernel

Sono state apportate diverse modifiche ai file system che il kernel di AL1 supporterà il montaggio, oltre a modifiche negli schemi di partizionamento che il kernel analizzerà.

Opzione **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_AFS_FS	m	n	n
CONFIG_AF_RXRPC	m	n	n
CONFIG_BSD_DISKLABEL	y	n	n
CONFIG_CRAMFS	m	n	n
CONFIG_CRAMFS_BLOCKDEV	N/D	N/D	N/D
CONFIG_DM_CLONE	N/D	n	n
CONFIG_DM_ERA	n	n	n
CONFIG_DM_INTEGRITY	m	m	m
CONFIG_DM_LOG_WRITES	n	m	m
CONFIG_DM_SWITCH	n	n	n
CONFIG_DM_VERITY	n	n	n
CONFIG_ECRYPT_FS	m	n	n
CONFIG_EXFAT_FS	N/D	m	m
CONFIG_EXT2_FS	m	n	n
CONFIG_EXT3_FS	m	n	n
CONFIG_GFS2_FS	n	n	n

Opzione **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_HFSPLUS_FS	m	n	n
CONFIG_HFS_FS	m	n	n
CONFIG_JFS_FS	m	n	n
CONFIG_LDM_PARTITION	y	n	n
CONFIG_MAC_PARTITION	y	n	n
CONFIG_NFS_V2	m	n	n
CONFIG_NTFS_FS	m	n	n
CONFIG_ROMFS_FS	m	n	n
CONFIG_SOLARIS_X86_PARTITION	y	n	n
CONFIG_SQUASHFS_ZSTD	y	y	y
CONFIG_SUN_PARTITION	y	n	n

Modifiche alla configurazione del kernel incentrate sulla sicurezza

Opzione **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_BUG_ON_DATA_CORRUPTION	y	y	y

Opzione **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_DEFAULT_MMAP_MIN_ADDR	4096	65536	65536
CONFIG_DEVMEM	y	n	n
CONFIG_DEVPORT	y	n	n
CONFIG_FORTIFY_SOURCE	y	y	y
CONFIG_HARDENED_USERCOPY_FALLBACK	N/D	N/D	N/D
CONFIG_INIT_ON_ALLOC_DEFAULT_ON	N/D	n	n
CONFIG_INIT_ON_FREE_DEFAULT_ON	N/D	n	n
CONFIG_IOMMU_DEFAULT_DMA_STRICT	N/D	n	n
CONFIG_LDISC_AUTOLOAD	y	n	n
CONFIG_SCHED_CORE	N/D	N/D	y
CONFIG_SCHED_STACK_END_CHECK	y	y	y

Opzione **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SECURITY_DMESG_RESTRICT	n	y	y
CONFIG_SECURITY_SELINUX_DISABLE	y	n	n
CONFIG_SHUFFLE_PAGE_ALLOCATOR	N/D	y	y
CONFIG_SLAB_FREELIST_HARDENED	y	y	y
CONFIG_SLAB_FREELIST_RANDOM	n	y	y

Altre modifiche apportate alla configurazione del kernel

Opzione **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_HZ	250	100	100
CONFIG_NR_CPUS	8192	512	512
CONFIG_PANIC_ON_OOPS	n	y	y
CONFIG_PANIC_ON_OOPS_VALUE	0	1	1

Opzione **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_PPP	m	n	n
CONFIG_SLIP	m	n	n
CONFIG_XEN_PV	y	N/D	n

Confronto dei pacchetti installati sulle AMI Amazon Linux 1 (AL1) e Amazon Linux 2023

Un confronto tra gli RPM presenti sulle AMI standard AL1 e AL2023.

Pacchetto	AMI AL1	AL2023 AMI
acl	2,2,49	2.3.1
acpid	2.0,19	2.0,32
alsa-lib	1,0,22	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-repo-s3		20233,20240219
amazon-linux-sb-keys		2023,1
amazon-rpm-config		228
amazon-ssm-agent	3,21705,0	3,22222,0
at	3,1,10	3,1,23
attr	2,4,46	2.5.1

Pacchetto	AMI AL1	AL2023 AMI
audit	2,6,5	30.6
audit-libs	2,6,5	30.6
authconfig	6.2.8	
aws-amitools-ec2	1,5,13	
aws-cfn-bootstrap	1.4	2.0
aws-cli	1,118,107	
awscli-2		2.14.5
basesystem	10,0	11
bash	4,2,46	5,2,15
bash-completion		2.11
bc	1,006,95	1,07,1
bind-libs	9,8,2	9,16,42
bind-license		9,16,42
bind-utils	9,82	9,16,42
binutils	2,27	2,39
boost-filesystem		1,75,0
boost-system		1,75,0
boost-thread		1,75,0
bzip2	1.0.6	1.0.8
bzip2-libs	1.0.6	1.0.8

Pacchetto	AMI AL1	AL2023 AMI
c-ares		1.19.0
ca-certificates	2023,2,62	2023,2,64
checkpolicy	2.1.10	3.4
chkconfig	1,349,3	1.15
chrony		4.3
cloud-disk-utils	0,27	
cloud-init	0,7,6	222,2
cloud-init-cfg-ec2		222,2
cloud-utils-growpart		0,31
copy-jdk-configs	3.3	
coreutils	8,22	8,32
coreutils-common		8,32
cpio	(2.10)	2,13
cracklib	2,8,16	2,9,6
cracklib-dicts	2,8,16	2,9,6
cronie	1.4.4	
cronie-anacron	1.4.4	
crontabs	1.10	1.11
crypto-policies		20220428
crypto-policies-scripts		20220428

Pacchetto	AMI AL1	AL2023 AMI
cryptsetup	1,6,7	2.6.1
cryptsetup-libs	1.6.7	2.6.1
curl	7,61,1	
curl-minimal		8,5,0
cyrus-sasl	2,1,23	
cyrus-sasl-lib	2,1,23	2,1,27
cyrus-sasl-plain	2,1,23	2,1,27
dash	0,5,5,1	
db4	4,7,25	
db4-utils	4,7,25	
dbus	1,6,12	1,12,28
dbus-broker		32
dbus-common		1,12,28
dbus-libs	1,6,12	1,12,28
dejavu-fonts-common	2,33	
dejavu-sans-fonts	2,33	
dejavu-serif-fonts	2,33	
device-mapper	1,02,135	1,02,185
device-mapper-event	1,02,135	
device-mapper-event-libs	1,02,135	

Pacchetto	AMI AL1	AL2023 AMI
device-mapper-libs	1,02,135	1,02,185
device-mapper-persistent-data	0,63	
dhclient	4.1.1	
dhcp-common	4.1.1	
diffutils	3.3	3.8
dmraid	1.0.0.rc16	
dmraid-events	1.0.0.rc16	
dnf		4.12.0
dnf-data		4.12.0
dnf-plugin-release-notification		1.2
dnf-plugin-support-info		1.2
dnf-plugins-core		4.1.0
dnf-utils		4.1.0
dosfstools		4.2
dracut	004	055
dracut-config-ec2		3.0
dracut-config-generic		055
dracut-modules-growroot	0.20	
dump	0.4	
dwz		0,14

Pacchetto	AMI AL1	AL2023 AMI
dyninst		102,1
e2fsprogs	1,43,5	1,46,5
e2fsprogs-libs	1,43,5	1,46,5
ec2-hibinit-agent	1.0.0	1.0.8
ec2-instance-connect		1.1
ec 2- instance-connect-selinux		1.1
ec2-net-utils	0.7	
ec2-utils	0.7	2.1.0
ed	1.1	1.14.2
efi-filesystem		5
efi-srpm-macros		5
efivar		38
efivar-libs		38
elfutils-debuginfod-client		0.188
elfutils-default-yama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libs		0.188
epel-release	6	
ethtool	3,15	5,15
expat	2.1.0	2.5.0

Pacchetto	AMI AL1	AL2023 AMI
file	5,37	5,39
file-libs	5,37	5,39
filesystem	2,4,30	3,14
findutils	44,2	4.8.0
fipscheck	1.3.1	
fipscheck-lib	1.3.1	
fontconfig	2.8.0	
fontpackages-filesystem	1,41	
fonts-srpm-macros		2.0.5
freetype	2,3,11	
fstrm		0.6.1
fuse-libs	2,9,4	2,9,9
gawk	3.1.7	5.1.0
gdbm	1.8.0	
gdbm-libs		1,19
gdisk	0,8,10	1.0.8
generic-logos	17,0	
get_reference_source	1.2	
gettext		0,21
gettext-libs		0,21

Pacchetto	AMI AL1	AL2023 AMI
ghc-srpm-macros		1.5.0
giflib	4.1.6	
glib2	2,36,3	2,74,7
glibc	2,17	2,34
glibc-all-langpacks		2,34
glibc-common	2,17	2,34
glibc-gconv-extra		2,34
glibc-locale-source		2,34
gmp	6.0.0	62,1
gnupg2	2.0,28	
gnupg2-minimal		2.3.7
gnutls		3.8.0
go-srpm-macros		3.2.0
gpgme	1.4.3	1.15.1
gpm-libs	1,20,6	1,20.7
grep	2,20	3.8
groff	1,22.2	
groff-base	1,22.2	1,22.4
grub	0,97	
grub2-common		2,06

Pacchetto	AMI AL1	AL2023 AMI
grub2-efi-x64-ec2		2,06
grub2-pc-modules		2,06
grub2-tools		2,06
grub2-tools-minimal		2,06
grubby	7,0,15	8,40
gssproxy		0.8.4
gzip	1.5	1.12
hesiod	3.1.0	
hibagent	1.0.0	
hmaccalc	0,9,12	
hostname		3,23
hunspell		1.7.0
hunspell-en		0,20140811,1
hunspell-en-GB		0,20140811,1
hunspell-en-US		0,20140811,1
hunspell-filesystem		1.7.0
hwdata	0,233	0,353
Info	5.1	6.7
inih		49
initscripts	9,03,58	10,09

Pacchetto	AMI AL1	AL2023 AMI
iproute	4.4.0	5.10.0
iptables	1,4,21	
iputils	20121221	20210202
irqbalance	1.5.0	1.9.0
jansson		2.14
java-1.7.0-openjdk	1,7,0,321	
javapackages-tools	0.9.1	
jitterentropy		3.4.1
jpackage-utils	1,7,5	
jq		1.6
json-c		0,14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4,148336	6,1,77
kernel-livepatch-repo-s3		20233,20240219
kernel-srpm-macros		1
kernel-tools	4,14,336	6,1,77
keyutils	1,5,8	1.6.3
keyutils-libs	1.5.8	1.6.3
kmod	14	29

Pacchetto	AMI AL1	AL2023 AMI
kmod-libs	14	29
kpartx	0,49	
kpatch-runtime		0,9,7
krb5-libs	1.15.1	1,21
lcms2	2.6	
less	436	608
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	2.3.1
libaio	0,3109	0,3111
libarchive		3,5,3

Pacchetto	AMI AL1	AL2023 AMI
libargon2		20171227
libassuan	2.0.3	2,5,5
libattr	2,4,46	2.5.1
libbasicobjects		0,11
libblkid	2,23,2	2,37,4
libcap	2,16	2,48
libcap-ng	0,7,5	0.8.2
libcap54	2,54	
libcbor		0.7.0
libcgroup	0,40 rc1	
libcollection		0.7.0
libcom_err	1,43,5	1,46,5
libcomps		0,1,18
libconfig		17.2
libcurl	7,61,1	
libcurl-minimal		8,5,0
libdb		5,3,28
libdhash		0,5,0
libdnf		0,67,0
libeconf		0,40

Pacchetto	AMI AL1	AL2023 AMI
libedit	2.11	3.1
libev		4,33
libevent	2.0,21	2,1,12
libfdisk		2,37,4
libffi	3,0,13	34.4
libfido2		1.10.0
libfontenc	1.0.5	
libgcc		114,1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.11	1,42
libgssglue	0.1	
libibverbs		37,0
libicu	50,2	
libidn	1,18	
libidn2	2.3.0	2.3.2
libini_config		1.3.1
libjpeg-turbo	1,2,90	
libkcapi		1.4.0

Pacchetto	AMI AL1	AL2023 AMI
libkcapi-hmaccalc		1.4.0
libldb		26.2
libmaxminddb		1.5.2
libmetalink		0,13
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2,23,2	2,37,4
libnetfilter_conntrack	1.0.4	
libnfnetlink	1.0.1	
libnfsidmap	0.25	2,5,4
libnghttp2	1,33,0	1,57,0
libnih	1.0.1	
libnl	1.1.4	
libnl3		3.5.0
libpath_utils		0,2,1
libpcap		1.10.1
libpipeline	1.2.3	1.5.3
libpkgconf		1.8.0
libpng	1,2,49	
libpsl	0.6.2	0,21,1

Pacchetto	AMI AL1	AL2023 AMI
libpwquality	1.2.3	1.4.4
libref_array		0,1,5
librepo		1.14.2
libreport-filesystem		2,15,2
libseccomp		2.5.3
libselinux	2.1.10	3.4
libselinux-utils	2.1.10	3.4
libsemanage	2.1.6	3.4
libsepol	2.1.7	3.4
libsigsegv		2,13
libsmartcols	2,23,2	2,37,4
libsolv		0,7,22
libss	1,43,5	1,46,5
libssh2	1.4.2	
libsss_certmap		2.5.0
libsss_idmap		2.5.0
libsss_nss_idmap		2.5.0
libstdc++		11.4.1
libstdc++72	7.2.1	
libstoragemgmt		1.9.4

Pacchetto	AMI AL1	AL2023 AMI
libsysfs	2.1.0	
libtalloc		2.3.4
libtasn1	2.3	4,19,0
libtdb		1.4.7
libtevent		0.13.0
libtextstyle		0,21
libtirpc	0,24	1.3.3
libudev	173	
libunistring	0,9,3	0,9,10
libuser	0,60	0,63
libutempter	1.1.5	1.2.1
libuuid	2,23,2	2,37,4
libuv		1.47.0
libverto	0,2,5	0,32
libverto-libev		0,32
libxcb	1.11	
libxcrypt		4,4,33
libxml2	2,9,1	210.4
libxml2-python27	29.1	
libxslt	1,1,28	

Pacchetto	AMI AL1	AL2023 AMI
libyaml	0,16	02,5
libzstd		1,5,5
lm_sensors-libs		3.6.0
lmdb-libs		0,9,29
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3,78	3,20,1
lsof	4,82	4,94,0
lua	5.1.4	
lua-libs		5.4.4
lua-srpm-macros		1
lvm2	2,02,166	
lvm2-libs	2,02,166	
lz4-libs		1.9.4
mailcap	2,1,31	
make	3,82	
man-db	26.3	29.3
man-pages	4,10	5,10
mdadm	3.2.6	
microcode_ctl	2.1	2.1
mingetty	1,08	

Pacchetto	AMI AL1	AL2023 AMI
mpfr		4.1.0
nano	2.5.3	5.8
nc	1,84	
ncurses	5.7	6.2
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
net-tools	1,60	2.0
nettle		3.8
newt	0,52,11	0,52,21
newt-python27	0,52,11	
nfs-utils	1.3.0	2,5,4
npth		1.6
nspr	4,25,0	4,35,0
nss	3,53,1	3,90,0
nss-pem	1.0.3	
nss-softokn	3,53,1	3,90,0
nss-softokn-freebl	3,53,1	3,90,0
nss-sysinit	3,53,1	3,90,0
nss-tools	3,53,1	
nss-util	3,53,1	3,90,0

Pacchetto	AMI AL1	AL2023 AMI
ntp	4.2.8 p15	
ntpdate	4.2.8p15	
ntsysv	1,349,3	1.15
numactl	2.0.7	
numactl-libs		2.0,14
ocaml-srpm-macros		6
oniguruma		6,9,7,1
openblas-srpm-macros		2
openldap	2,4,40	2,4,57
openssh	7,4p 1	8,7p1
openssh-clients	7,4p1	8,7p1
openssh-server	7,4p1	8,7p1
openssl	1,0,2k	3,0,8
openssl-libs		30,8
openssl-pkcs11		0,4,12
os-prober		1,77
p11-kit	0,18,5	0,24,1
p11-kit-trust	0,18,5	0,24,1
package-notes-srpm-macros		0.4
pam	1.1.8	1.5.1

Pacchetto	AMI AL1	AL2023 AMI
pam_ccreds	10	
pam_krb5	2,3,11	
pam_passwdqc	1.0.5	
parted	2.1	3.4
passwd	0,79	0,80
pciutils	3,1,10	3.7.0
pciutils-libs	3,1,10	3.7.0
pcre	8,21	
pcre2		10,40
pcre2-syntax		10,40
perl	5,16,3	
perl-Carp	1,26	1,50
perl-Class-Struct		0,66
perl-Digest	1,17	
perl-Digest-HMAC	1,03	
perl-Digest-MD5	2,52	
perl-Digest-SHA	5,85	
perl- DynaLoader		1,47
perl-Encode	2,51	3,15
perl-Errno		1,30

Pacchetto	AMI AL1	AL2023 AMI
perl-Exporter	5,68	5,74
perl-Fcntl		1.13
perl-File-Basename		2,85
perl-File-Path	2,09	2,18
perl-File-Temp	0,23,01	0,231,100
perl-File-stat		1,09
perl-Filter	1,49	
perl-Getopt-Long	2,40	2,52
perl-Getopt-Std		1.12
perl-HTTP-Tiny	0,033	0,078
perl-IO		1,43
perl-IPC-Open3		1,21
perl-MIME-Base64		3,16
perl-POSIX		1,94
perl- PathTools	3,40	3,78
perl-Pod-Escapes	1.04	1,07
perl-Pod-Perldoc	3,20	3,28,01
perl-Pod-Simple	3,28	3,42
perl-Pod-Usage	1,63	2,01
perl-Scalar-List-Utils	1,27	1,56

Pacchetto	AMI AL1	AL2023 AMI
perl- SelectSaver		1.02
perl-Socket	2.010	2,032
perl-Storable	2,45	3,21
perl-Symbol		1,08
perl-Term-ANSIColor		5,01
perl-Term-Cap		1,17
Testo in Perl- ParseWords	3.29	3,30
perl-Text-Tabs+Wrap		2021,0726
Tempo Perl- HiRes	1,9725	
perl-Time-Local	1,2300	1.300
perl-constant	1,27	1,33
perl-if		0,60,800
perl-interpreter		5,32,1
perl-libs	5,16,3	5,32,1
perl-macros	5,16,3	
perl-mro		1,23
perl-overload		1,31
perl-overloading		0,02
perl-parent	0,225	0,238
perl-podlators	2.5.1	4,14

Pacchetto	AMI AL1	AL2023 AMI
perl-srpm-macros		1
perl-subs		1,03
perl-threads	1,87	
perl-threads-shared	1,43	
perl-vars		1,05
pinentry	0,7,6	
pkgconf		1.8.0
pkgconf-m4		1.8.0
pkgconf-pkg-config		1.8.0
pkgconfig	0,27,1	
pm-utils	1.4.1	
policycoreutils	2,1,12	3.4
policycoreutils-python-utils		3.4
popt	1.13	1,18
procmail	3,22	
procps	32,8	
procps-ng		3,3,17
protobuf-c		1.4.1
psacct	6,32	6.6.4
psmisc	22,20	23,4

Pacchetto	AMI AL1	AL2023 AMI
pth	2.0.7	
publicsuffix-list-dafsa		20221208
python-chevron		0.13.1
python-srpm-macros		3.9
python27	2,7,18	
python27-PyYAML	3,10	
python27-babel	0.9.4	
python27-backports	1	
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	

Pacchetto	AMI AL1	AL2023 AMI
python27-futures	3.0.3	
python27-imaging	1.1.6	
python27-iniparse	0,31	
python27-jinja2	27.2	
python27-jmespath	0.9.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1	
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	

Pacchetto	AMI AL1	AL2023 AMI
python27-requests	1.2.3	
python27-rsa	3.4.1	
python27-setuptools	36,27	
python27-simplejson	3.6.5	
python27-six	1.8.0	
python27-urlgrabber	3,10	
python27-urllib3	1,24,3	
python27-virtualenv	15,10	
python3		3,9,16
python3-attrs		20,3,0
python3-audit		30.6
python3-awscrt		0,19,19
python3-babel		2,9,1
python3-cffi		1,14,5
python3-chardet		4.0.0
python3-colorama		04.4
python3-configobj		50.6
python3-cryptography		36,0
python3-daemon		2.3.0
python3-dateutil		28.1

Pacchetto	AMI AL1	AL2023 AMI
python3-dbus		1,2,18
python3-distro		1.5.0
python3-dnf		4.12.0
python 3- dnf-plugins-core		4.1.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0,67,0
python3-idna		(2.10)
python3-jinja2		211.3
python3-jmespath		0.10.0
python3-jsonpatch		1,21
python3-jsonpointer		2.0
python3-jsonschema		3.2.0
python3-libcomps		0,1,18
python3-libdnf		0,67,0
python3-libs		3,9,16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-libstoragemgmt		1.9.4
python3-lockfile		0.12.2

Pacchetto	AMI AL1	AL2023 AMI
python3-markupsafe		1.1.1
python3-netifaces		0,10,6
python3-oauthlib		3.0.2
python3-pip-wheel		21,31
python3-ply		3,11
python3-policycoreutils		3.4
python3-prettytable		0.7.2
python3-prompt-toolkit		3,0,24
python3-pycparser		2,20
python3-pyrsistent		0,17,3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022,7,1
python3-pyyaml		5.4.1
python3-requests		2,25,1
python3-rpm		4,161,3
python3-ruamel-yaml		0,16,6
pitone 3- ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59,6,0

Pacchetto	AMI AL1	AL2023 AMI
python3-setuptools-wheel		59,6,0
python3-six		1.15.0
python3-urllib3		1,25,10
python3-wcwidth		0,2,5
quota	4,00	4,06
quota-nls	4,00	4,06
readline	6.2	8.1
rmt	0.4	
rng-tools	5	6,14
rootfiles	8.1	8.1
rpcbind	0,2,0	1.2.6
rpm	4.11.3	4,161,3
rpm-build-libs	4.11,3	4,161,3
rpm-libs	4.11,3	4,161,3
rpm-plugin-selinux		4,161,3
rpm-plugin-systemd-inhibit		4,161,3
rpm-python27	4.11,3	
rpm-sign-libs		4,161,3
rsync	30.6	3.2.6
rsyslog	5,8,10	

Pacchetto	AMI AL1	AL2023 AMI
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	
rust-srpm-macros		21
sbsigntools		0.9.4
screen	40,3	4.8.0
sed	4.2.1	4.8
selinux-policy		37,22
selinux-policy-targeted		37,22
sendmail	8,14,4	
setserial	2,17	
setup	2,8,14	2,13,7
sgpio	1,2,0,10	
shadow-utils	4,14.2	4.9

Pacchetto	AMI AL1	AL2023 AMI
shared-mime-info	1.1	
slang	2.2.1	2.3.2
sqlite	3,7,17	
sqlite-libs		3,4,0
sssd-client		2.5.0
sssd-common		2.5.0
sssd-kcm		2.5.0
strace		5,16
sudo	1,8,23	1,9,14
sysctl-defaults	1.0	1
sysfsutils	2.1.0	
sysstat		12,5,6
system-release	2018,03	20233,20240219
systemd		252,16
systemd-libs		252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-udev		252,16
systemtap-runtime		4,8

Pacchetto	AMI AL1	AL2023 AMI
sysvinit	2,87	
tar	1,26	1,34
tbb		2020,3
tcp_wrappers	7.6	
tcp_wrappers-libs	7.6	
tcpdump		4,99,1
tcsh		6,24,07
time	1,7	1.9
tmpwatch	2,9,16	
traceroute	2.0,14	2.1.3
ttmkfdir	3,09	
tzdata	2023 c	2024a
tzdata-java	2023c	
udev	173	
unzip	6.0	6.0
update-motd	1.0.1	2.1
upstart	0,6,5	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2,23,2	2,37,4

Pacchetto	AMI AL1	AL2023 AMI
util-linux-core		2,37,4
vim-common	9,0,2120	9,0,2153
vim-data	9,0,2120	9,0,2153
vim-enhanced	9,0,2120	9,0,2153
vim-filesystem	9,0,2120	9,0,2153
vim-minimal	9,0,2120	9,0,2153
wget	1,18	1,21,3
which	2,19	2,21
words	3.0	3.0
xfsdump		3,1,11
xfsprogs		5,18,0
xorg-x11-font-utils	7.2	
xorg-x11-fonts-Type1	7.2	
xxd	9,0,2120	9,0,2153
xxhash-libs		0.8.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.12.0
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1,1,31	

Pacchetto	AMI AL1	AL2023 AMI
yum-plugin-upgrade-helper	1,1,31	
yum-utils	1,1,31	
zip	3.0	3.0
zlib	1.2.8	1,2,11
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1,5,5

Confronto dei pacchetti installati sulle AMI minime Amazon Linux 1 (AL1) e Amazon Linux 2023

Un confronto tra gli RPM presenti sulle AMI minimali AL1 e AL2023.

Pacchetto	AL1 Minimal	AL2023 Minimo
acpid	2.0.19	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-repo-s3		20233,20240219
amazon-linux-sb-keys		2023,1
audit	2,6,5	30.6
audit-libs	2,6,5	30.6

Pacchetto	AL1 Minimal	AL2023 Minimo
authconfig	6.2.8	
awscli-2		2.14.5
basesystem	10,0	11
bash	4,2,46	5,2,15
binutils	2,27	
bzip2	1.0.6	
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,62	2023,2,64
checkpolicy	2.1.10	3.4
chkconfig	1,349,3	
chrony		4.3
cloud-disk-utils	0,27	
cloud-init	0,7,6	222,2
cloud-init-cfg-ec2		222,2
cloud-utils-growpart		0,31
coreutils	8,22	8,32
coreutils-common		8,32
cpio	(2.10)	2,13
cracklib	2,8,16	2,9,6
cracklib-dicts	2,8,16	2,9,6

Pacchetto	AL1 Minimal	AL2023 Minimo
cronie	1.4.4	
cronie-anacron	1.4.4	
crontabs	1.10	
crypto-policies		20220428
cryptsetup-libs		2.6.1
curl	7,61,1	
curl-minimal		8,5,0
cyrus-sasl	2,1,23	
cyrus-sasl-lib	2,1,23	2,1,27
dash	0,5,5,1	
db4	4,7,25	
db4-utils	4,7,25	
dbus		1,12,28
dbus-broker		32
dbus-common		1,12,28
dbus-libs	1,6,12	1,12,28
device-mapper		1,02,185
device-mapper-libs		1,02,185
dhclient	4.1.1	
dhcp-common	4.1.1	

Pacchetto	AL1 Minimal	AL2023 Minimo
diffutils	3.3	3.8
dnf		4.12.0
dnf-data		4.12.0
dnf-plugin-release-notification		1.2
dnf-plugin-support-info		1.2
dnf-plugins-core		4.1.0
dracut	004	055
dracut-config-ec2		3.0
dracut-config-generic		055
dracut-modules-growroot	0.20	
e2fsprogs	1,43,5	1,46,5
e2fsprogs-libs	1,43,5	1,46,5
ec2-utils	0.7	2.1.0
ed	1.1	
efi-filesystem		5
efivar		38
efivar-libs		38
elfutils-default-yama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libs		0.188

Pacchetto	AL1 Minimal	AL2023 Minimo
ethtool	3,15	
expat	2.1.0	2.5.0
file	5,37	5,39
file-libs	5,37	5,39
filesystem	2,4,30	3,14
findutils	44,2	4.8.0
fipscheck	1.3.1	
fipscheck-lib	1.3.1	
fuse-libs	2,9,4	2,9,9
gawk	3.1.7	5.1.0
gdbm	1.8.0	
gdbm-libs		1,19
gdisk	0,8,10	1.0.8
generic-logos	17,0	
get_reference_source	1.2	
gettext		0,21
gettext-libs		0,21
glib2	2,36,3	2,74,7
glibc	2,17	2,34
glibc-all-langpacks		2,34

Pacchetto	AL1 Minimal	AL2023 Minimo
glibc-common	2,17	2,34
glibc-locale-source		2,34
gmp	6.0.0	62,1
gnupg2	2.0,28	
gnupg2-minimal		2.3.7
gnutls		3.8.0
gpgme	1.4.3	1.15.1
grep	2,20	3.8
groff	1,22.2	
groff-base	1,22.2	1,22.4
grub	0,97	
grub2-common		2,06
grub2-efi-x64-ec2		2,06
grub2-pc-modules		2,06
grub2-tools		2,06
grub2-tools-minimal		2,06
grubby	7,0,15	8,40
gzip	1.5	1.12
hesiod	3.1.0	
hmaccalc	0,9,12	

Pacchetto	AL1 Minimal	AL2023 Minimo
hostname		3,23
hwdata	0,233	0,353
Info	5.1	
inih		49
initscripts	9,03,58	10,09
iproute	4.4.0	5.10.0
iptables	1,4,21	
iputils	20121221	20210202
irqbalance		1.9.0
jansson		2.14
jitterentropy		3.4.1
jq		1.6
json-c		0,14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4,14,336	6,1,77
kernel-livepatch-repo-s3		20233,20240219
keyutils-libs	1,5,8	1.6.3
kmod	14	29
kmod-libs	14	29

Pacchetto	AL1 Minimal	AL2023 Minimo
krb5-libs	1.15.1	1,21
less	436	608
libacl	2,2,49	2.3.1
libarchive		3,5,3
libargon2		20171227
libassuan	2.0.3	2,5,5
libattr	2,4,46	2.5.1
libblkid	2,23,2	2,37,4
libcap	2,16	2,48
libcap-ng	0,7,5	0.8.2
libcap54	2,54	
libcbor		0.7.0
libcgroup	0,40. rc1	
libcom_err	1,43,5	1,46,5
libcomps		0,1,18
libcurl	7,61,1	
libcurl-minimal		8,5,0
libdb		5,3,28
libdnf		0,67,0
libeconf		0,40

Pacchetto	AL1 Minimal	AL2023 Minimo
libedit	2.11	3.1
libfdisk		2,37,4
libffi	3,0,13	34.4
libfido2		1.10.0
libgcc		11.4.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.11	1,42
libicu	50,2	
libidn	1,18	
libidn2	2.3.0	2.3.2
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2,23,2	2,37,4
libnetfilter_conntrack	1.0.4	
libnfnetlink	1.0.1	
libnghttp2	1,33,0	1,57,0

Pacchetto	AL1 Minimal	AL2023 Minimo
libnih	1.0.1	
libpipeline		1.5.3
libpsl	0.6.2	
libpwquality	1.2.3	1.4.4
librepo		1.14,2
libreport-filesystem		2,15,2
libseccomp		2.5.3
libselinux	2.1.10	3.4
libselinux-utils	2.1.10	3.4
libsemanage	2.1.6	3.4
libsepol	2.1.7	3.4
libsigsegv		2,13
libsmartcols	2,23,2	2,37,4
libsolv		0,7,22
libss	1,43,5	1,46,5
libssh2	1.4.2	
libstdc++		11.4.1
libstdc++72	7.2.1	
libsysfs	2.1.0	
libtasn1	2.3	4,19,0

Pacchetto	AL1 Minimal	AL2023 Minimo
libtextstyle		0,21
libudev	173	
libunistring	0,9,3	0,9,10
libuser	0,60	0,63
libutempter	1.1.5	1.2.1
libuuid	2,23,2	2,37,4
libverto	0,2,5	0,32
libxcrypt		4,4,33
libxml2	2,9,1	210.4
libyaml	0,16	02,5
libzstd		1,5,5
logrotate	3,7,8	3,20,1
lua	5.1.4	
lua-libs		5.4.4
lz4-libs		1.9.4
make	3,82	
man-db		2,9,3
microcode_ctl	2.1	2.1
mingetty	1,08	
mpfr		4.1.0

Pacchetto	AL1 Minimal	AL2023 Minimo
ncurses	5.7	6.2
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
net-tools	1,60	2.0
nettle		3.8
newt	0,52,11	
newt-python27	0,52,11	
npth		1.6
nspr	4,25,0	
nss	3,53,1	
nss-pem	1.0.3	
nss-softokn	3,53,1	
nss-softokn-freebl	3,53,1	
nss-sysinit	3,53,1	
nss-tools	3,53,1	
nss-util	3,53,1	
ntp	4.2.8 p15	
ntpdate	4.2.8p15	
numactl-libs		2.0,14
oniguruma		6,9,7,1

Pacchetto	AL1 Minimal	AL2023 Minimo
openldap	2,4,40	2,4,57
openssh	7,4p 1	8,7p1
openssh-clients		8,7p1
openssh-server	7,4p1	8,7p1
openssl	1,0,2k	3,0,8
openssl-libs		30,8
openssl-pkcs11		0,4,12
os-prober		1,77
p11-kit	0,18,5	0,24,1
p11-kit-trust	0,18,5	0,24,1
pam	1.1.8	1.5.1
passwd	0,79	0,80
pciutils	3,1,10	3.7.0
pciutils-libs	3,1,10	3.7.0
pcre	8,21	
pcre2		10,40
pcre2-syntax		10,40
pinentry	0,7,6	
pkgconfig	0,27,1	
policycoreutils	2,1,12	3.4

Pacchetto	AL1 Minimal	AL2023 Minimo
popt	1.13	1,18
procmail	3,22	
procps	32,8	
procps-ng		3,3,17
psmisc	22,20	23,4
pth	2.0.7	
python27	2,7,18	
python27-PyYAML	3,10	
python27-babel	0.9.4	
python27-backports	1	
python27-backports-ssl_match_hostname	3,40,2	
python27-chardet	2.0.1	
python27-configobj	4,7,2	
python27-iniparse	0,31	
python27-jinja2	27.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1	
python27-libs	2,7,18	
python27-markupsafe	0,11	
python27-pycurl	7,19,0	

Pacchetto	AL1 Minimal	AL2023 Minimo
python27-pygpgme	0.3	
python27-pyliblzma	0,5,3	
python27-pyxattr	0,5,0	
python27-requests	1.2.3	
python27-setuptools	36,27	
python27-six	1.8.0	
python27-urlgrabber	3,10	
python27-urllib3	1,24,3	
python3		3,9,16
python3-attrs		20,3,0
python3-audit		30.6
python3-awscrt		0,19,19
python3-babel		2,9,1
python3-cffi		1,14,5
python3-chardet		4.0.0
python3-colorama		04.4
python3-configobj		50.6
python3-cryptography		36,0
python3-dateutil		28.1
python3-dbus		1,2,18

Pacchetto	AL1 Minimal	AL2023 Minimo
python3-distro		1.5.0
python3-dnf		4.12.0
python 3- dnf-plugins-core		4.1.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0,67,0
python3-idna		(2.10)
python3-jinja2		211.3
python3-jmespath		0.10.0
python3-jsonpatch		1,21
python3-jsonpointer		2.0
python3-jsonschema		3.2.0
python3-libcomps		0,1,18
python3-libdnf		0,67,0
python3-libs		3,9,16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-markupsafe		1.1.1
python3-netifaces		0,10,6
python3-oauthlib		3.0.2

Pacchetto	AL1 Minimal	AL2023 Minimo
python3-pip-wheel		21,31
python3-ply		3,11
python3-policycoreutils		3.4
python3-prettytable		0.7.2
python3-prompt-toolkit		3,0,24
python3-pycparser		2,20
python3-pyrsistent		0,17,3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022,7,1
python3-pyyaml		5.4.1
python3-requests		2,25,1
python3-rpm		4,161,3
python3-ruamel-yaml		0,16,6
pitone 3- ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59,60
python3-setuptools-wheel		59,6,0
python3-six		1.15.0
python3-urllib3		1,25,10

Pacchetto	AL1 Minimal	AL2023 Minimo
python3-wcwidth		0,2,5
readline	6.2	8.1
rng-tools		6,14
rootfiles	8.1	8.1
rpm	4.11.3	4,161,3
rpm-build-libs	411,3	4,161,3
rpm-libs	411,3	4,161,3
rpm-plugin-selinux		4,161,3
rpm-plugin-systemd-inhibit		4,161,3
rpm-python27	411,3	
rpm-sign-libs		4,161,3
rsyslog	5,8,10	
sbsigntools		0.9.4
sed	42,1	4.8
selinux-policy		37,22
selinux-policy-targeted		37,22
sendmail	8,14,4	
setserial	2,17	
setup	2,8,14	2,13,7
shadow-utils	4.1.4.2	4.9

Pacchetto	AL1 Minimal	AL2023 Minimo
shared-mime-info	1.1	
slang	2.2.1	
sqlite	3,7,17	
sqlite-libs		3,4,0
sudo	1,8,23	1,9,14
sysctl-defaults	1.0	1
sysfsutils	2.1.0	
system-release	2018,03	20233,20240219
systemd		252,16
systemd-libs		252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-udev		252,16
sysvinit	2,87	
tar	1,26	1,34
tcp_wrappers-libs	7.6	
tzdata	2023 c	2024a
udev	173	
update-motd	1.0.1	2.1

Pacchetto	AL1 Minimal	AL2023 Minimo
upstart	0,6,5	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2,23,2	2,37,4
util-linux-core		2,37,4
vim-data	9,0,2120	9,0,2153
vim-minimal	9,0,2120	9,0,2153
which	2,19	2,21
xfsprogs		5,18,0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.12.0
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1,1,31	
yum-plugin-upgrade-helper	1,1,31	
zlib	1.2.8	1,2,11
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1,5,5

Confronto dei pacchetti installati sulle immagini dei container di base Amazon Linux 1 (AL1) e Amazon Linux 2023

Un confronto tra gli RPM presenti nelle immagini dei container base AL1 e AL2023.

Pacchetto	Contenitore AL1	Contenitore AL2023
alternatives		1.15
amazon-linux-repo-cdn		20233,20240219
audit-libs		3,0,6
basesystem	10,0	11
bash	4,2,46	5,2,15
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,62	2023,2,64
chkconfig	1,349,3	
coreutils	8,22	
coreutils-single		8,32
crypto-policies		20220428
curl	7,61,1	
curl-minimal		8,5,0
cyrus-sasl-lib	2,1,23	
db4	4,7,25	
db4-utils	4,7,25	
dnf		4.12.0

Pacchetto	Contenitore AL1	Contenitore AL2023
dnf-data		4.12.0
elfutils-default-yama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libs		0.188
expat	2.1.0	2.5.0
file-libs	5,37	5,39
filesystem	2,4,30	3,14
gawk	3.1.7	5.1.0
gdbm	1.8.0	
gdbm-libs		1,19
glib2	2,36,3	2,74,7
glibc	2,17	2,34
glibc-common	2,17	2,34
glibc-minimal-langpack		2,34
gmp	6.0.0	62,1
gnupg2	2.0,28	
gnupg2-minimal		2.3.7
gpgme	1.4.3	1.15.1
grep	2,20	3.8
gzip	1.5	

Pacchetto	Contenitore AL1	Contenitore AL2023
Info	5.1	
json-c		0,14
keyutils-libs	1.5.8	1.6.3
krb5-libs	1.15.1	1,21
libacl	2,2,49	2.3.1
libarchive		3,5,3
libassuan	2.0.3	2,5,5
libattr	2,4,46	2.5.1
libblkid		2,37,4
libcap	2,16	2,48
libcap-ng		0.8.2
libcom_err	1,43,5	1,46,5
libcomps		0,1,18
libcurl	7,61,1	
libcurl-minimal		8,5,0
libdnf		0,67,0
libffi	3,0,13	34.4
libgcc		114,1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2

Pacchetto	Contenitore AL1	Contenitore AL2023
libgomp		11.4.1
libgpg-error	1.11	1,42
libicu	50,2	
libidn2	2.3.0	2.3.2
libmodulemd		2.13.0
libmount		2,37,4
libnghttp2	1,33,0	1,57,0
libpsl	0.6.2	
librepo		1.14,2
libreport-filesystem		2,15,2
libselinux	2.1.10	3.4
libsepol	2.1.7	3.4
libsigsegv		2,13
libsmartcols		2,37,4
libsolv		0,7,22
libssh2	1.4.2	
libstdc++		11,4,1
libstdc++72	7.2.1	
libtasn1	2.3	4,19,0
libunistring	0,9,3	0,9,10

Pacchetto	Contenitore AL1	Contenitore AL2023
libuuid		2,37,4
libverto	0,2,5	0,32
libxcrypt		4,4,33
libxml2	2,9,1	210.4
libxml2-python27	29.1	
libyaml		0,2,5
libzstd		1,5,5
lua	5.1.4	
lua-libs		5.4.4
lz4-libs		1.9.4
make	3,82	
mpfr		4.1.0
ncurses	5.7	
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
npth		1.6
nspr	4,25,0	
nss	3,53,1	
nss-pem	1.0.3	
nss-softokn	3,53,1	

Pacchetto	Contenitore AL1	Contenitore AL2023
nss-softokn-freebl	3,53,1	
nss-sysinit	3,53,1	
nss-tools	3,53,1	
nss-util	3,53,1	
openldap	2,4,40	
openssl	1,0,2k	
openssl-libs		3,0,8
p11-kit	0,18,5	0,24,1
p11-kit-trust	0,18,5	0,24,1
pcre	8,21	
pcre2		10,40
pcre2-syntax		10,40
pinentry	0,7,6	
pkgconfig	0,27,1	
popt	1.13	1,18
pth	2.0.7	
python27	2,7,18	
python27-chardet	2.0.1	
python27-iniparse	0,31	
python27-kitchen	1.1.1	

Pacchetto	Contenitore AL1	Contenitore AL2023
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	
python3		3,9,16
python3-dnf		4.12.0
python3-gpg		1.15.1
python3-hawkey		0,67,0
python3-libcomps		0,1,18
python3-libdnf		0,67,0
python3-libs		3,9,16
python3-pip-wheel		21,31
python3-rpm		4,16,1,3
python3-setuptools-wheel		59,60
readline	6.2	8.1
rpm	411,3	4,161,3
rpm-build-libs	411,3	4,161,3
rpm-libs	411,3	4,161,3

Pacchetto	Contenitore AL1	Contenitore AL2023
rpm-python27	411,3	
rpm-sign-libs		4,161,3
sed	42,1	4.8
setup	2,8,14	2,13,7
shared-mime-info	1.1	
sqlite	3,7,17	
sqlite-libs		3,4,0
sysctl-defaults	1	
system-release	2018,03	20233,20240219
tar	1,26	
tzdata	2023 c	2024a
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.12.0
yum-metadata-parser	1.1.4	
yum-plugin-ovl	1,1,31	
yum-plugin-priorities	1,1,31	
yum-utils	1,1,31	
zlib	1.2.8	1,2,11

Requisiti di sistema AL2023

Questa sezione descrive i requisiti di sistema per l'utilizzo di AL2023.

Argomenti

Requisiti della CPU per l'esecuzione di AL2023

Per eseguire qualsiasi codice AL2023, il processore utilizzato deve soddisfare determinati requisiti minimi. I tentativi di eseguire AL2023 su CPU che non soddisfano questi requisiti potrebbero causare errori di istruzione illegali nelle prime fasi dell'esecuzione del codice.

I requisiti minimi si applicano a AL2023 su Amazon EC2AL2023 nei container, e. AL2023 al di fuori di Amazon EC2

Requisiti della CPU ARM per AL2023

Tutti i file binari AL2023 `aarch64` (ARM) sono progettati per 64 bit. Non sono disponibili ARM file binari a 32 bit, quindi è necessaria una CPU a 64 bitARM.

> **Note**
>
> Per le istanze basate su ARM, AL2023 supporta solo i tipi di istanza che utilizzano processori Graviton2 o successivi. AL2023 non supporta le istanze A1.

AL2023 richiede un processore compatibile con ARMv8.2 con Cryptography Extension (`ARMv8.2+crypto`). Tutti i pacchetti AL2023 per `aarch64` sono compilati con il flag del `-march=armv8.2-a+crypto` compilatore. Sebbene cerchiamo di stampare messaggi di errore corretti quando si tenta di eseguire il codice AL2023 su ARM processori più vecchi, è possibile che il primo messaggio di errore sia un errore di istruzione illegale.

> **Note**
>
> A causa dei requisiti di `aarch64` base della CPU AL2023, tutti i Raspberry Pi sistemi precedenti a AL2023 Raspberry Pi 5 non soddisfano i requisiti minimi della CPU.

Requisiti della CPU x86-64 per AL2023

Tutti i `x86-64` binari AL2023 sono creati per la `x86-64v2` revisione dell'`x86-64`architettura - `march=x86-64-v2` passandoli al compilatore.

La `x86-64v2` revisione dell'architettura aggiunge le seguenti funzionalità della CPU all'architettura di base: `x86-64`

- `CMPXCHG16B`
- `LAHF-SAHF`
- `POPCNT`
- `SSE3`
- `SSE4_1`
- `SSE4_2`
- `SSSE3`

Ciò corrisponde approssimativamente ai `x86-64` processori rilasciati nel 2009 o successivamente. Gli esempi includonoIntel Nehalem,AMD Jaguar,Atom Silvermont, insieme alle VIA Nano e Eden C microarchitetture.

In Amazon EC2, tutti i tipi di istanze `x86-64` supportano `x86-64v2`, incluse le famiglie di istanze `M1`, `C1` e `M2`.

Non vengono creati file binari x86 (i686) AL2023 a 32 bit. Sebbene AL2023 mantenga il supporto per l'esecuzione di file binari dello spazio utente a 32 bit, questa funzionalità è obsoleta e potrebbe essere rimossa in una futura versione principale di Amazon Linux. Per ulteriori informazioni, consulta Pacchetti x86 (i686) a 32 bit.

Requisiti di memoria (RAM) per l'esecuzione di AL2023

La `.nano` famiglia di tipi di istanze Amazon EC2 (`t2.nano`, `t3.nanot3a.nano`, `et4g.nano`) dispone di 512 MB di RAM, che è il requisito minimo per AL2023.

> **Note**
>
> Sebbene il requisito minimo sia 512 MB, questi tipi di istanze hanno limiti di memoria e funzionalità e prestazioni potrebbero essere limitate.

Le immagini AL2023 non sono state testate su sistemi con meno di 512 MB di RAM. L'esecuzione di immagini di container basate su AL2023 in meno di 512 MB di RAM dipenderà dal carico di lavoro containerizzato.

Alcuni carichi di lavoro, ad esempio `dnf update` tra alcune versioni di AL2023, possono richiedere più di 512 MB di RAM. Per questo motivo, la versione AL2023.3 ha introdotto l'abilitazione per impostazione `zram` predefinita per le istanze con meno di 800 MB di RAM. Per i carichi di lavoro containerizzati, ciò significa che alcuni carichi di lavoro potrebbero funzionare correttamente su istanze AL2023 con questa quantità di memoria, ma fallire se eseguiti in un contenitore con un utilizzo limitato a questa quantità di memoria.

Per i tipi di istanza con meno di 800 MB di RAM, AL2023 (a partire da AL2023.3 o versioni successive) abiliterà lo scambio basato su `zram` per impostazione predefinita. Esempi di tipi di istanze Amazon EC2 con meno di 800 MB di memoria includono`t4g.nano`, `t3a.nano` `t3.nanot2.nano`, e. `t1.micro` Ciò comporta un minor numero di scenari di memoria insufficiente per questi tipi di istanza, dal momento che AL2023 comprime e decomprime le pagine di memoria on demand. In questo modo, vengono abilitati i carichi di lavoro che altrimenti richiederebbero un tipo di istanza con più memoria, a scapito dell'utilizzo della CPU che serve per eseguire la compressione.

Utilizzo di AL2023 su AWS

Puoi configurare AL2023 per utilizzarlo con altri. Servizi AWS Ad esempio, puoi scegliere un'AMI AL2023 quando avvii un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

Per queste procedure di configurazione, utilizzi il servizio AWS Identity and Access Management (IAM). Per informazioni complete su IAM, consulta i seguenti materiali di riferimento:

- AWS Identity and Access Management (IAM)
- Guida per l'utente di IAM

Argomenti

Iniziare con AWS

Iscriviti a un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo la registrazione Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente amministratore.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Concessione dell'accesso programmatico

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con l' AWS AWS Management Console esterno di. Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste	Segui le istruzioni in Uso delle credenziali temporanee con

Quale utente necessita dell'accesso programmatico?	Per	Come
	programmatiche agli SDK o alle API AWS CLI. AWS AWS	AWS risorse nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimento agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

AL2023 su Amazon EC2

Utilizza una delle seguenti procedure per avviare un'istanza Amazon EC2 con un'AMI AL2023. Puoi scegliere l'AMI standard o l'AMI minima. Per ulteriori informazioni sulle differenze tra AMI standard e AMI minima, consulta Confronto tra le AMI AL2023 standard (predefinite) e minime.

Argomenti

- Avvio di AL2023 utilizzando la console Amazon EC2
- Avvio di AL2023 utilizzando il parametro SSM e AWS CLI
- Lancio dell'ultima AMI AL2023 utilizzando AWS CloudFormation

- Avvio di AL2023 utilizzando un ID AMI specifico
- Deprecazione e ciclo di vita dell'AMI AL2023
- Connessione alle istanze AL2023
- Confronto tra AMI standard e minime AL2023

Avvio di AL2023 utilizzando la console Amazon EC2

Usa la console Amazon EC2 per avviare un'AMI AL2023.

> **Note**
>
> Per le istanze basate su ARM, AL2023 supporta solo i tipi di istanza che utilizzano processori Graviton2 o successivi. AL2023 non supporta le istanze A1.

Attieniti ai passaggi seguenti per avviare un'istanza Amazon EC2 con un'AMI AL2023 dalla console Amazon EC2.

Per avviare un'istanza EC2 con un'AMI AL2023

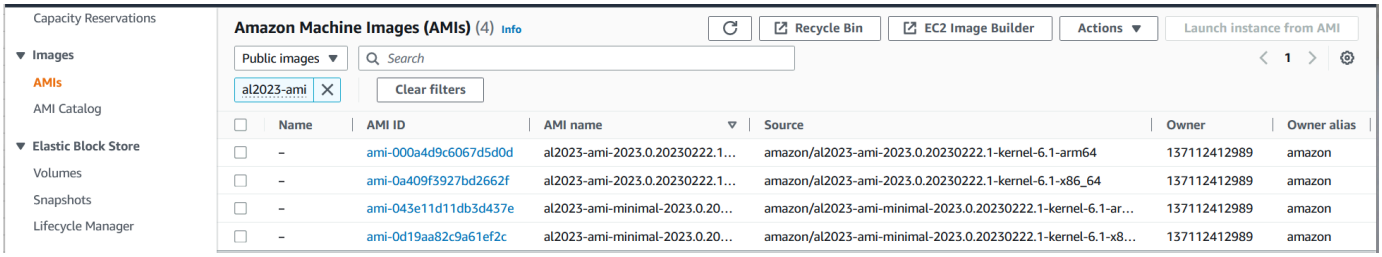
1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Scegli Immagini pubbliche nel menu a discesa.
4. Inserisci **`al2023-ami`** nel campo di ricerca.

   > **Note**
   >
   > Assicurati che la dicitura amazon compaia nella colonna Alias owner.

5. Seleziona un'immagine dall'elenco. Sotto Origine, puoi determinare se l'AMI è standard o minima. Il nome di un'AMI AL2023 può essere interpretato utilizzando questo formato:

   ```
   'al2023-[ami || ami-minimal]-2023.0.[release build date].[build
   number]-kernel-[version number]-[arm64 || x86_64]'
   ```

6. L'immagine seguente mostra un elenco parziale delle AMI AL2023.



Per ulteriori informazioni sull'avvio delle istanze Amazon EC2, consulta Nozioni di base sulle istanze Amazon EC2 Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Avvio di AL2023 utilizzando il parametro SSM e AWS CLI

In AWS CLI, è possibile utilizzare il valore del parametro SSM di un'AMI per avviare una nuova istanza di AL2023. Più specificamente, usa uno dei valori dinamici del parametro SSM inclusi nel seguente elenco e aggiungi `/aws/service/ami-amazon-linux-latest/` prima del valore del parametro SSM. Questo ti consente di avviare l'istanza nell'interfaccia AWS CLI.

- `al2023-ami-kernel-default-arm64` per l'architettura arm64
- `al2023-ami-minimal-kernel-default-arm64` per l'architettura arm64 (AMI minima)
- `al2023-ami-kernel-default-x86_64` per l'architettura x86_64
- `al2023-ami-minimal-kernel-default-x86_64` per l'architettura x86_64 (AMI minima)

> **Note**
>
> Ciascuno degli elementi in *`corsivo`* è un parametro di esempio. Sostituiscili con le tue informazioni.

```
$ aws ec2 run-instances \
  --image-id \
    resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
  --instance-type m5.xlarge \
  --region us-east-1 \
  --key-name aws-key-us-east-1 \
  --security-group-ids sg-004a7650
```

Il flag `--image-id` specifica il valore del parametro SSM.

Il flag `--instance-type` specifica il tipo e le dimensioni dell'istanza. Questo flag deve essere compatibile con il tipo di AMI selezionato.

Il `--region` flag specifica Regione AWS dove crei l'istanza.

Il `--key-name` flag specifica la chiave Regione AWS che viene utilizzata per connettersi all'istanza. Se non fornisci una chiave esistente nella regione in cui crei l'istanza, non puoi connetterti all'istanza tramite SSH.

Il flag `--security-group-ids` specifica il gruppo di sicurezza che determina le autorizzazioni di accesso per il traffico di rete in entrata e in uscita.

> **Important**
>
> È AWS CLI necessario specificare un gruppo di sicurezza esistente che consenta l'accesso all'istanza dal computer remoto tramite portaTCP:22. Senza un gruppo di sicurezza specificato, la nuova istanza viene inserita in un gruppo di sicurezza predefinito. In un gruppo di sicurezza predefinito, l'istanza può connettersi solo alle altre istanze all'interno del tuo VPC.

Per ulteriori informazioni, consulta Avvio, elencazione e chiusura delle istanze Amazon EC2 nella Guida per l'utente di AWS Command Line Interface .

Lancio dell'ultima AMI AL2023 utilizzando AWS CloudFormation

Per avviare un'AMI AL2023 utilizzando AWS CloudFormation, utilizza uno dei seguenti modelli.

> **Note**
>
> Ciascuna delle AMI `Arm64` e `x86_64` richiede tipi di istanza diversi. Per ulteriori informazioni consultare Tipi di istanza Amazon EC2

Modello `JSON`:

```
{
  "Parameters": {
    "LatestAmiId": {
      "Type": "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
      "Default": "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-
default-x86_64"
```

```
    }
  },
  "Resources": {
    "MyEC2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "InstanceType": "t2.large",
        "ImageId": {
          "Ref": "LatestAmiId"
        }
      }
    }
  }
}
```

Modello YAML:

```
Parameters:
  LatestAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-default-
x86_64'

Resources:
  Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      InstanceType: 't2.large'
      ImageId: !Ref LatestAmiId
```

Assicurati di sostituire il parametro AMI alla fine della sezione "Predefinito", se necessario. Sono disponibili i seguenti valori di parametri:

- `al2023-ami-kernel-6.1-arm64` per l'architettura arm64
- `al2023-ami-minimal-kernel-6.1-arm64` per l'architettura arm64 (AMI minima)
- `al2023-ami-kernel-6.1-x86_64` per l'architettura x86_64
- `al2023-ami-minimal-kernel-6.1-x86_64` per l'architettura x86_64 (AMI minima)

Di seguito sono riportate le specifiche dinamiche del kernel. La versione predefinita del kernel cambia automaticamente con ogni aggiornamento della versione principale del kernel.

- `al2023-ami-kernel-default-arm64` per l'architettura arm64
- `al2023-ami-minimal-kernel-default-arm64` per l'architettura arm64 (AMI minima)
- `al2023-ami-kernel-default-x86_64` per l'architettura x86_64
- `al2023-ami-minimal-kernel-default-x86_64` per l'architettura x86_64 (AMI minima)

Avvio di AL2023 utilizzando un ID AMI specifico

Puoi avviare un'AMI AL2023 specifica utilizzando l'ID AMI. Puoi determinare l'ID AMI AL2023 necessaria consultando l'elenco delle AMI nella console Amazon EC2. Oppure puoi usare. AWS Systems Manager Se usi Systems Manager, assicurati di selezionare l'alias AMI tra quelli elencati nella sezione precedente. Per ulteriori informazioni, consulta Query per gli ID AMI Amazon Linux più recenti utilizzando AWS Systems Manager Parameter Store.

Deprecazione e ciclo di vita dell'AMI AL2023

Ogni nuovo rilascio di AL2023 include una nuova AMI. Al momento della registrazione, l'AMI viene contrassegnata con una data di obsolescenza. La data di obsolescenza per ciascuna AMI AL2023 è di 90 giorni dal momento del relativo rilascio, affinché il periodo corrisponda a quello per cui l'Applicazione di patch Kernel Live su AL2023 è offerta per ogni singolo rilascio del kernel.

> **Note**
>
> La data di obsolescenza di 90 giorni si riferisce a una singola AMI e non alla Cadenza di rilascio di AL2023 o al periodo di supporto del prodotto.

Per ulteriori informazioni sulla dichiarazione delle AMI come obsolete, consulta la pagina dedicata all'obsolescenza delle AMI nella Guida per l'utente di Amazon EC2 per le istanze Linux.

L'uso regolare di un'AMI aggiornata per avviare un'istanza garantisce che quest'ultima venga avviata con i più recenti aggiornamenti di sicurezza, incluso un kernel aggiornato. Se avvii una versione precedente di un'AMI e poi applichi gli aggiornamenti, esiste un periodo di tempo per cui l'istanza non dispone dei più recenti aggiornamenti di sicurezza. Per assicurarti di utilizzare l'AMI più recente, ti consigliamo di usare i parametri SSM.

Per ulteriori informazioni sull'uso dei parametri SSM per avviare un'istanza, consulta:

- Avvio di AL2023 utilizzando il parametro SSM e AWS CLI

- Lancio dell'ultima AMI AL2023 utilizzando AWS CloudFormation

Connessione alle istanze AL2023

Usa SSH o AWS Systems Manager per connetterti alla tua istanza AL2023.

Connettersi all'istanza tramite SSH

Per istruzioni su come connettersi a un'istanza tramite SSH, consulta Connessione a un'istanza Linux tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Connect alla tua istanza utilizzando AWS Systems Manager

Per istruzioni su come utilizzare la connessione AWS Systems Manager a un'istanza AL2023, consulta Connettiti alla tua istanza Linux utilizzando Session Manager nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Utilizzo di Amazon EC2 Instance Connect

L'AMI AL2023, esclusa l'AMI minima, viene fornita con l'agente EC2 Instance Connect installato per impostazione predefinita. Per utilizzare EC2 Instance Connect con un'istanza AL2023 lanciata dall'AMI minima, è necessario installare il `ec2-instance-connect` pacchetto. Per istruzioni sull'uso di EC2 Instance Connect, consulta Connessione a un'istanza Linux con EC2 Instance Connect nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Confronto tra AMI standard e minime AL2023

Puoi avviare un'istanza Amazon EC2 con un'AMI AL2023 standard (predefinita) o minima. Per istruzioni su come avviare un'istanza Amazon EC2 con il tipo di AMI standard o minimo, consulta. AL2023 su Amazon EC2

L'AMI AL2023 standard include tutte le applicazioni e gli strumenti più comunemente usati installati. Consigliamo di usare l'AMI standard se desideri iniziare rapidamente e non ti interessa personalizzare l'AMI.

L'AMI AL2023 minima è la versione di base semplificata che contiene solo gli strumenti e le utilità di base necessari per eseguire il sistema operativo (OS). Consigliamo di usare l'AMI minima se desideri avere il minor ingombro possibile del sistema operativo. L'AMI minima offre un utilizzo leggermente ridotto dello spazio su disco e una migliore efficienza in termini di costi a lungo termine. L'AMI minima è adatta se desideri un sistema operativo più piccolo e hai problemi a installare manualmente strumenti e applicazioni.

L'immagine di container è più simile all'AMI minima AL2023 nel set di pacchetti.

Confronto dei pacchetti installati sulle immagini Amazon Linux 2023

Un confronto tra gli RPM presenti nelle immagini AL2023 AMI, Minimal AMI e Container.

Pacchetto	AMI	AMI minima	Container
acl	2.3.1		
acpid	2.0.32		
alternatives	1.15	1.15	1.15
amazon-chrony-config	4.3	4.3	
amazon-ec2-net-utils	2.4.1	2.4.1	
amazon-linux-repo-cdn			2023,420240319
amazon-linux-repo-s3	2023,420240319	2023,420240319	
amazon-linux-sb-keys	2023,1	2023,1	
amazon-rpm-config	228		
amazon-ssm-agent	3,2,2303,0		
at	3,1,23		
attr	2.5.1		
audit	30,6	30.6	
audit-libs	30.6	30.6	30.6
aws-cfn-bootstrap	2.0		
awscli-2	2.14.5	2.14.5	
basesystem	11	11	11

Pacchetto	AMI	AMI minima	Container
bash	5,2,15	5,2,15	5,2,15
bash-completion	2.11		
bc	1,07,1		
bind-libs	9,16,48		
bind-license	9,16,48		
bind-utils	9,16,48		
binutils	2,39		
boost-filesystem	1,75,0		
boost-system	1,75,0		
boost-thread	1,75,0		
bzip2	1.0.8		
bzip2-libs	1.0.8	1.0.8	1.0.8
c-ares	1.19.0		
ca-certificates	2023,2,64	2023,2,64	2023,2,64
checkpolicy	3.4	3.4	
chkconfig	1.15		
chrony	4.3	4.3	
cloud-init	222,2	222,2	
cloud-init-cfg-ec2	222,2	222,2	
cloud-utils-growpart	0,31	0,31	

Pacchetto	AMI	AMI minima	Container
coreutils	8,32	8,32	
coreutils-common	8,32	8,32	
coreutils-single			8,32
cpio	2,13	2,13	
cracklib	2,9,6	29.6	
cracklib-dicts	29.6	29.6	
crontabs	1.11		
crypto-policies	20220428	20220428	20220428
crypto-policies-scripts	20220428		
cryptsetup	2.6.1		
cryptsetup-libs	2.6.1	2.6.1	
curl-minimal	8,5,0	8,5,0	8,5,0
cyrus-sasl-lib	2,1,27	2,1,27	
cyrus-sasl-plain	2,1,27		
dbus	1,12,28	1,12,28	
dbus-broker	32	32	
dbus-common	1,12,28	1,12,28	
dbus-libs	1,12,28	1,12,28	
device-mapper	1,02,185	1,02,185	
device-mapper-libs	1,02,185	1,02,185	

Pacchetto	AMI	AMI minima	Container
diffutils	3.8	3.8	
dnf	4.14.0	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2	
dnf-plugin-support-info	1.2	1.2	
dnf-plugins-core	4.3.0	4.3.0	
dnf-utils	4.3.0		
dosfstools	4.2		
dracut	055	055	
dracut-config-ec2	3.0	3.0	
dracut-config-generic	055	055	
dwz	0,14		
dyninst	102,1		
e2fsprogs	1,446,5	1,46,5	
e2fsprogs-libs	1,46,5	1,46,5	
ec2-hibinit-agent	1.0.8		
ec2-instance-connect	1.1		
ec 2- instance-connect-selinux	1.1		
ec2-utils	2.2.0	2.2.0	

Pacchetto	AMI	AMI minima	Container
ed	1.14.2		
efi-filesystem	5	5	
efi-srpm-macros	5		
efivar	38	38	
efivar-libs	38	38	
elfutils-debuginfod-client	0.188		
elfutils-default-yama-scope	0.188	0.188	0.188
elfutils-libelf	0.188	0.188	0.188
elfutils-libs	0.188	0.188	0.188
ethtool	5,15		
expat	2.5.0	2.5.0	2.5.0
file	5,39	5,39	
file-libs	5,39	5,39	5,39
filesystem	3,14	3,14	3,14
findutils	4.8.0	4.8.0	
fonts-srpm-macros	2.0.5		
fstrm	0.6.1		
fuse-libs	2,9,9	29.9	
gawk	5.1.0	5.1.0	5.1.0

Pacchetto	AMI	AMI minima	Container
gdbm-libs	1,19	1,19	1,19
gdisk	1.0.8	1.0.8	
gettext	0,21	0,21	
gettext-libs	0,21	0,21	
ghc-srpm-macros	1.5.0		
glib2	2,74,7	2,74,7	2,74,7
glibc	2,34	2,34	2,34
glibc-all-langpacks	2,34	2,34	
glibc-common	2,34	2,34	2,34
glibc-gconv-extra	2,34		
glibc-locale-source	2,34	2,34	
glibc-minimal-lang pack			2,34
gmp	62,1	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7	2.3.7
gnutls	3.8.0	3.8.0	
go-srpm-macros	3.2.0		
gpgme	1.15.1	1.15.1	1.15.1
gpm-libs	1,20.7		
grep	3.8	3.8	3.8
groff-base	1,22,4	1,22,4	

Pacchetto	AMI	AMI minima	Container
grub2-common	2,06	2,06	
grub2-efi-aa64-ec2	2,06 (aarch64)	2.06 (aarch64)	
grub2-efi-x64-ec2	2,06 (x86_64)	2,06 (x86_64)	
grub2-pc-modules	2,06	2,06	
grub2-tools	2,06	2,06	
grub2-tools-minimal	2,06	2,06	
grubby	8,40	8,40	
gssproxy	0.8.4		
gzip	1.12	1.12	
hostname	3,23	3,23	
hunspell	1.7.0		
hunspell-en	0,20140811,1		
hunspell-en-GB	0,20140811,1		
hunspell-en-US	0,20140811,1		
hunspell-filesystem	1.7.0		
hwdata	0,3353	0,3353	
Info	6.7		
inih	49	49	
initscripts	10,09	10,09	
iproute	5.10.0	5.10.0	

Pacchetto	AMI	AMI minima	Container
iputils	20210202	20210202	
irqbalance	1.9.0	1.9.0	
jansson	2.14	2.14	
jitterentropy	3.4.1	3.4.1	
jq	1.7.1	1.7.1	
json-c	0,14	0,14	0,14
kbd	2.4.0	2.4.0	
kbd-misc	2.4.0	2.4.0	
kernel	61,79	6,1,79	
kernel-livepatch-repo-s3	2023,420240319	2023,420240319	
kernel-srpm-macros	1		
kernel-tools	6,1,79		
keyutils	1.6.3		
keyutils-libs	1.6.3	1.6.3	1.6.3
kmod	29	29	
kmod-libs	29	29	
kpatch-runtime	0,9,7		
krb5-libs	1,21	1,21	1,21
less	608	608	
libacl	2.3.1	2.3.1	2.3.1

Pacchetto	AMI	AMI minima	Container
libaio	0,3111		
libarchive	3,5,3	3,5,3	3,5,3
libargon2	20171227	20171227	
libassuan	2,5,5	2,5,5	2,5,5
libattr	2.5.1	2.5.1	2.5.1
libbasicobjects	0,11		
libblkid	2,37,4	2,37,4	2,37,4
libcap	2,48	2,48	2,48
libcap-ng	0.8.2	0.8.2	0.8.2
libcbor	0.7.0	0.7.0	
libcollection	0.7.0		
libcom_err	1,446,5	1,46,5	1,46,5
libcomps	01,20	01,20	01,20
libconfig	17.2		
libcurl-minimal	8,5,0	8,5,0	8,5,0
libdb	5,3,28	5,3,28	
libdhash	0,5,0		
libdnf	0,69,0	0,69,0	0,69,0
libeconf	0,40	0,40	
libedit	3.1	3.1	

Pacchetto	AMI	AMI minima	Container
libev	4,33		
libevent	2,1,12		
libfdisk	2,37,4	2,37,4	
libffi	34.4	34.4	34.4
libfido2	1.10.0	1.10.0	
libgcc	114,1	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2	1.10.2
libgomp	11.4.1	11.4.1	11.4.1
libgpg-error	1,42	1,42	1,42
libibverbs	48,0		
libidn2	2.3.2	2.3.2	2.3.2
libini_config	1.3.1		
libkcapi	1.4.0	1.4.0	
libkcapi-hmaccalc	1.4.0	1.4.0	
libldb	26.2		
libmaxminddb	1.5.2		
libmetalink	0,13		
libmnl	1.0.4	1.0.4	
libmodulemd	2.13.0	2.13.0	2.13.0
libmount	2,37,4	2,37,4	2,37,4

Pacchetto	AMI	AMI minima	Container
libnfsidmap	2,5,4		
libnghttp2	1,57,0	1,57,0	1,57,0
libnl3	3.5.0		
libpath_utils	0,2,1		
libpcap	1.10.1		
libpipeline	1.5.3	1.5.3	
libpkgconf	1.8.0		
libpsl	0,21,1	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4	
libref_array	0,1,5		
librepo	1,14,5	1,14,5	1,14,5
libreport-filesystem	2,15,2	2,15,2	2,15,2
libseccomp	2.5.3	2.5.3	
libselinux	3.4	3.4	3.4
libselinux-utils	3.4	3.4	
libsemanage	3.4	3.4	
libsepol	3.4	3.4	3.4
libsigsegv	2,13	2,13	2,13
libsmartcols	2,37,4	2,37,4	2,37,4
libsolv	0,7,22	0,7,22	0,7,22

Pacchetto	AMI	AMI minima	Container
libss	1,446,5	1,46,5	
libsss_certmap	2,9,4		
libsss_idmap	2,9,4		
libsss_nss_idmap	2,9,4		
libsss_sudo	2.9.4		
libstdc++	11.4.1	11.4.1	11.4.1
libstoragemgmt	1.9.4		
libtalloc	2.3.4		
libtasn1	4,19,0	4,19,0	4,19,0
libtdb	1.4.7		
libtevent	0.13.0		
libtextstyle	0,21	0,21	
libtirpc	1.3.3		
libunistring	0,9,10	0,9,10	0,9,10
libuser	0,63	0,63	
libutempter	1.2.1	1.2.1	
libuuid	2,37,4	2,37,4	2,37,4
libuv	1.47.0		
libverto	0,32	0,32	0,32
libverto-libev	0,32		

Pacchetto	AMI	AMI minima	Container
libxcrypt	4,4,33	4,4,33	4,4,33
libxml2	2,10,4	210.4	210.4
libyaml	02,5	02,5	02,5
libzstd	1,5,5	1,5,5	1,5,5
lm_sensors-libs	3.6.0		
lmdb-libs	0,9,29		
logrotate	3,20,1	3,20,1	
lsof	4,94,0		
lua-libs	5.4.4	5.4.4	5.4.4
lua-srpm-macros	1		
lz4-libs	1.9.4	1.9.4	1.9.4
man-db	2,9,3	29.3	
man-pages	5,10		
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)	
mpfr	4.1.0	4.1.0	4.1.0
nano	5.8		
ncurses	6.2	6.2	
ncurses-base	6.2	6.2	6.2
ncurses-libs	6.2	6.2	6.2
net-tools	2.0	2.0	

Pacchetto	AMI	AMI minima	Container
nettle	3.8	3.8	
newt	0,52,21		
nfs-utils	2,5,4		
npth	1.6	1.6	1.6
nspr	4,35,0		
nss	3,90,0		
nss-softokn	3,90,0		
nss-softokn-freebl	3,90,0		
nss-sysinit	3,90,0		
nss-util	3,90,0		
ntsysv	1.15		
numactl-libs	2.0,14	2.0,14	
ocaml-srpm-macros	6		
oniguruma	6,9,7,1	6,9,7,1	
openblas-srpm-macros	2		
openldap	2,4,57	2,4,57	
openssh	8.7p1	8,7p1	
openssh-clients	8,7p1	8,7p1	
openssh-server	8,7p1	8,7p1	
openssl	3,0,8	30,8	

Pacchetto	AMI	AMI minima	Container
openssl-libs	30,8	30,8	30,8
openssl-pkcs11	0,4,12	0,4,12	
os-prober	1,77	1,77	
p11-kit	0,24,1	0,24,1	0,24,1
p11-kit-trust	0,24,1	0,24,1	0,24,1
package-notes-srpm-macros	0.4		
pam	1.5.1	1.5.1	
parted	3.4		
passwd	0,80	0,80	
pciutils	3.7.0	3.7.0	
pciutils-libs	3.7.0	3.7.0	
pcre2	10,40	10,40	10,40
pcre2-syntax	10,40	10,40	10,40
perl-Carp	1,50		
perl-Class-Struct	0,66		
perl- DynaLoader	1,47		
perl-Encode	3,15		
perl-Errno	1,30		
perl-Exporter	5,74		
perl-Fcntl	1.13		

Pacchetto	AMI	AMI minima	Container
perl-File-Basename	2,85		
perl-File-Path	2,18		
perl-File-Temp	0,231,100		
perl-File-stat	1,09		
perl-Getopt-Long	2,52		
perl-Getopt-Std	1.12		
perl-HTTP-Tiny	0,078		
perl-IO	1,43		
perl-IPC-Open3	1,21		
perl-MIME-Base64	3,16		
perl-POSIX	1,94		
perl- PathTools	3,78		
perl-Pod-Escapes	1,07		
perl-Pod-Perldoc	3,28,01		
perl-Pod-Simple	3,42		
perl-Pod-Usage	2,01		
perl-Scalar-List-Utils	1,56		
perl- SelectSaver	1.02		
perl-Socket	2.032		
perl-Storable	3,21		

Pacchetto	AMI	AMI minima	Container
perl-Symbol	1,08		
perl-Term-ANSIColor	5,01		
perl-Term-Cap	1,17		
Testo in Perl-ParseWords	3.30		
perl-Text-Tabs+Wrap	2021,0726		
perl-Time-Local	1,300		
perl-constant	1,33		
perl-if	0,60,800		
perl-interpreter	5,32,1		
perl-libs	5,32,1		
perl-mro	1,23		
perl-overload	1,31		
perl-overloading	0,02		
perl-parent	0,238		
perl-podlators	4,14		
perl-srpm-macros	1		
perl-subs	1,03		
perl-vars	1,05		
pkgconf	1.8.0		
pkgconf-m4	1.8.0		

Pacchetto	AMI	AMI minima	Container
pkgconf-pkg-config	1.8.0		
policycoreutils	3.4	3.4	
policycoreutils-python-utils	3.4		
popt	1,18	1,18	1,18
procps-ng	3,3,17	3,3,17	
protobuf-c	1.4.1		
psacct	6,6,4		
psmisc	23,4	23,4	
publicsuffix-list-dafsa	20240212	20240212	20240212
python-chevron	0.13.1		
python-srpm-macros	3.9		
python3	3,9,16	3,9,16	3,9,16
python3-attrs	20,3,0	20,3,0	
python3-audit	30.6	3.0.6	
python3-awscrt	0,19,19	0,19,19	
python3-babel	2,9,1	29.1	
python3-cffi	1,14,5	1,14,5	
python3-chardet	4.0.0	4.0.0	
python3-colorama	04.4	04.4	
python3-configobj	50.6	5.0.6	

Pacchetto	AMI	AMI minima	Container
python3-cryptography	36,0	36,0	
python3-daemon	2.3.0		
python3-dateutil	28.1	28.1	
python3-dbus	1,2,18	1,2,18	
python3-distro	1.5.0	1.5.0	
python3-dnf	4.14.0	4.14.0	4.14.0
python 3- dnf-plugins-core	4.3.0	4.3.0	
python3-docutils	0,16	0,16	
python3-gpg	1.15.1	1.15.1	1.15.1
python3-hawkey	0,69,0	0,69,0	0,69,0
python3-idna	(2.10)	(2.10)	
python3-jinja2	211,3	2.11.3	
python3-jmespath	0.10.0	0.10.0	
python3-jsonpatch	1,21	1,21	
python3-jsonpointer	2.0	2.0	
python3-jsonschema	3.2.0	3.2.0	
python3-libcomps	01,20	01,20	01,20
python3-libdnf	0,69,0	0,69,0	0,69,0
python3-libs	3,9,16	3,9,16	3,9,16
python3-libselinux	3.4	3.4	

Pacchetto	AMI	AMI minima	Container
python3-libsemanage	3.4	3.4	
python3-libstorage mgmt	1.9.4		
python3-lockfile	0.12.2		
python3-markupsafe	1.1.1	1.1.1	
python3-netifaces	0,10,6	0,10,6	
python3-oauthlib	3.0.2	3.0.2	
python3-pip-wheel	21,31	21,31	21,31
python3-ply	3,11	3,11	
python3-policycore utils	3.4	3.4	
python3-prettytable	0.7.2	0.7.2	
python3-prompt-toolkit	3,0,24	3,0,24	
python3-pycparser	2,20	2,20	
python3-pyrsistent	0,17,3	0,17,3	
python3-pyserial	3.4	3.4	
python3-pysocks	1.7.1	1.7.1	
python3-pytz	2022,7,1	2022,7,1	
python3-pyyaml	5.4.1	5.4.1	
python3-requests	2,25,1	2,25,1	
python3-rpm	4,161,3	4,161,3	4,161,3

Pacchetto	AMI	AMI minima	Container
python3-ruamel-yaml	0,16,6	0,16,6	
pitone 3- ruamel-yaml-clib	0.1.2	0,1,2	
python3-setools	4.4.1	4.4.1	
python3-setuptools	59,60	59,6,0	
python3-setuptools-wheel	59,6,0	59,6,0	59,6,0
python3-six	1.15.0	1.15.0	
sistema python3	235	235	
python3-urllib3	1,25,10	1,25,10	
python3-wcwidth	0,2,5	02,5	
quota	4,06		
quota-nls	4,06		
readline	8.1	8.1	8.1
rng-tools	6,14	6,14	
rootfiles	8.1	8.1	
rpcbind	1.2.6		
rpm	4,16,13	4,161,3	4,161,3
rpm-build-libs	4,161,3	4,161,3	4,161,3
rpm-libs	4,161,3	4,161,3	4,161,3
rpm-plugin-selinux	4,161,3	4,161,3	

Pacchetto	AMI	AMI minima	Container
rpm-plugin-systemd-inhibit	4,161,3	4,161,3	
rpm-sign-libs	4,161,3	4,161,3	4,161,3
rsync	3.2.6		
rust-srpm-macros	21		
sbsigntools	0.9.4	0.9.4	
screen	4.8.0		
sed	4.8	4.8	4.8
selinux-policy	37,22	37,22	
selinux-policy-targeted	37,22	37,22	
setup	2,13,7	2,13,7	2,13,7
shadow-utils	4.9	4.9	
slang	2.3.2		
sqlite-libs	3,4,0	3,4,0	3,4,0
sssd-client	2,9,4		
sssd-common	2,9,4		
sssd-kcm	2,9,4		
sssd-nfs-idmap	2,9,4		
strace	5,16		
sudo	1,9,14	1,9,14	

Pacchetto	AMI	AMI minima	Container
sysctl-defaults	1.0	1	
sysstat	12,5,6		
system-release	2023,420240319	2023,420240319	2023,420240319
systemd	252,16	252,16	
systemd-libs	252,16	252,16	
systemd-networkd	252,16	252,16	
systemd-pam	252,16	252,16	
systemd-resolved	252,16	252,16	
systemd-udev	252,16	252,16	
systemtap-runtime	4,8		
tar	1,34	1,34	
tbb	2020,3		
tcpdump	4,99,1		
tcsh	6,24,07		
time	1.9		
traceroute	2.1.3		
tzdata	2024a	2024a	2024a
unzip	6.0		
update-motd	2.2	2.2	
userspace-rcu	0.12.1	0.12.1	

Pacchetto	AMI	AMI minima	Container
util-linux	2,37,4	2,37,4	
util-linux-core	2,37,4	2,37,4	
vim-common	9,0,2153		
vim-data	9,0,2153	9,0,2153	
vim-enhanced	9,0,2153		
vim-filesystem	9,0,2153		
vim-minimal	9,0,2153	9,0,2153	
wget	1,21,3		
which	2,21	2,21	
words	3.0		
xfsdump	3,1,11		
xfsprogs	5,18,0	5,18,0	
xxd	9,0,2153		
xxhash-libs	0.8.0		
xz	52,5	5.2.5	
xz-libs	5.2.5	5.2.5	5.2.5
yum	4.14.0	4.14.0	4.14.0
zip	3.0		
zlib	1,2,11	1,2,11	1,2,11
zram-generator	1.1.2	1.1.2	

Pacchetto	AMI	AMI minima	Container
zram-generator-defaults	1.1.2	1.1.2	
zstd	1,5,5	1,5,5	

Utilizzo di AL2023 in contenitori

> **Note**
>
> Per ulteriori informazioni su come utilizzare AL2023 per ospitare carichi di lavoro containerizzati su Amazon ECS, consulta. AL2023 per host di container Amazon ECS

Esistono diversi modi in cui AL2023 può essere utilizzato all'interno dei contenitori, a seconda del caso d'uso. Immagine di container di base AL2023È molto simile a un'immagine di contenitore Amazon Linux 2 e all'AMI minima AL2023.

Per gli utenti esperti, offriamo un'immagine minima del contenitore, introdotta nella versione AL2023.2, insieme alla documentazione che descrive come creare contenitori bare-bone.

AL2023 può essere utilizzato anche per l'hosting dei carichi di lavoro containerizzati, sia di immagini di container basate su AL2023 sia di container basati su altre distribuzioni Linux. Puoi usare AL2023 per host di container Amazon ECS oppure usare direttamente i pacchetti di runtime dei container forniti. I pacchetti `docker`, `containerd` e `nerdctl` sono disponibili per essere installati e utilizzati su AL2023.

Argomenti

- Utilizzo dell'immagine del contenitore di base AL2023
- Immagine minima del contenitore AL2023
- Creazione di immagini minime di contenitori AL2023
- Confronto dei pacchetti installati sulle immagini di container Amazon Linux 2023
- Confronto dei pacchetti installati sulle immagini di container e AMI minime Amazon Linux 2023

Utilizzo dell'immagine del contenitore di base AL2023

L'immagine del contenitore AL2023 è costruita con gli stessi componenti software inclusi nell'AMI AL2023. È disponibile per l'uso in qualsiasi ambiente come immagine di base per i carichi di lavoro di Docker. Se usi già l'AMI Amazon Linux per le applicazioni in Amazon Elastic Compute Cloud (Amazon EC2), puoi containerizzare le tue applicazioni con l'immagine di container Amazon Linux.

Usa l'immagine del contenitore Amazon Linux nel tuo ambiente di sviluppo locale e poi invia l'applicazione all' AWS utilizzo di Amazon Elastic Container Service (Amazon ECS). Per ulteriori informazioni, consulta la pagina dedicata all'utilizzo di immagini Amazon ECR con Amazon ECS nella Guida per l'utente di Amazon Elastic Container Registry.

L'immagine di container Amazon Linux è disponibile su Amazon ECR Public. Puoi fornire un feedback per AL2023 tramite il tuo AWS rappresentante designato o segnalando un problema nel repository amazon-linux-2023 su. GitHub

Per estrarre l'immagine di container Amazon Linux da Amazon ECR Public

1. Autentica il client Docker nel registro Amazon Linux Public. I token di autenticazione sono validi 12 ore. Per ulteriori informazioni, consulta Autenticazione del registro privato nella Guida per l'utente di Amazon Elastic Container Registry.

   > **Note**
   >
   > Il get-login-password comando è supportato dall'ultima versione della versione 2. AWS CLI Per ulteriori informazioni, consulta Installazione dell' AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface .

   ```
   $ aws ecr-public get-login-password --region us-east-1 | docker login --username
    AWS --password-stdin public.ecr.aws
   ```

   L'output è il seguente.

   ```
   Login succeeded
   ```

2. Estrai l'immagine di container Amazon Linux eseguendo il comando docker pull. Per visualizzare l'immagine del container Amazon Linux nella galleria di Amazon ECR Public, consulta la galleria di Amazon ECR Public - amazonlinux.

> **Note**
>
> Quando estrai l'immagine di container Docker AL2023, puoi usare i tag in uno dei seguenti formati:
>
> - Per ottenere la versione più recente dell'immagine di container AL2023, usa il tag `:2023`.
> - Per ottenere una versione specifica di AL2023, puoi usare il seguente formato:
>   - `:2023.`*`[0-7 release quarter]`*`.`*`[release date]`*`.`*`[build number]`*
>
> Gli esempi seguenti usano il tag `:2023` ed estraggono l'immagine di container più recente disponibile di AL2023.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023
```

3. (Opzionale) Esegui il container a livello locale.

```
$ docker run -it --security-opt seccomp=unconfined public.ecr.aws/amazonlinux/
amazonlinux:2023 /bin/bash
```

Per estrarre l'immagine di container da Docker Hub

1. Estrai l'immagine di container AL2023 con il comando docker pull.

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

2. (Opzionale) Esegui il container a livello locale.

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

> **Note**
>
> L'immagine di container AL2023 usa solo lo strumento di gestione dei pacchetti `dnf` per installare i pacchetti software. Ciò significa che non esiste alcun comando `amazon-linux-extras` né uno equivalente da usare per software aggiuntivi.

Immagine minima del contenitore AL2023

> **Note**
>
> Le immagini standard del contenitore AL2023 sono adatte alla maggior parte dei casi d'uso e l'adattamento all'immagine minima del contenitore è probabilmente più faticoso che adattarsi all'immagine del contenitore di base AL2023.

L'immagine minima del contenitore AL2023, introdotta in AL2023.2, si differenzia dall'immagine del contenitore di base perché contiene solo i pacchetti minimi necessari per installare altri pacchetti. L'immagine minima del contenitore è progettata per essere un insieme minimo di pacchetti, non un comodo set di pacchetti.

L'immagine di container minima AL2023 è sviluppata a partire da componenti software già disponibili in AL2023. La differenza principale nell'immagine minimale del contenitore consiste nell'`microdnf`utilizzare il gestore di `dnf` pacchetti piuttosto che quello Python basato su tutte le funzionalità`dnf`. Ciò consente di ridurre l'immagine minima del contenitore, con il vantaggio di non disporre del set completo di funzionalità del gestore di `dnf` pacchetti, incluso nelle AMI AL2023 e nell'immagine del contenitore di base.

L'immagine minimale del contenitore AL2023 costituisce la base dell'ambiente di runtime `provided.al2023` AWS Lambda.

Per un elenco dettagliato dei pacchetti inclusi nell'immagine minima del contenitore, vedi. Confronto dei pacchetti installati sulle immagini di container Amazon Linux 2023

Dimensioni dell'immagine di container minima

Poiché l'immagine minima del contenitore AL2023 contiene meno pacchetti rispetto all'immagine del contenitore di base AL2023, è anche significativamente più piccola. La tabella seguente confronta le opzioni relative all'immagine del contenitore delle versioni correnti e precedenti di Amazon Linux.

> **Note**
>
> Le dimensioni delle immagini sono quelle mostrate nella pagina della Galleria pubblica di Amazon ECR dedicata ad Amazon Linux.

Immagine	Versione	Dimensioni dell'immagine	Nota
Amazon Linux 1 (AL1)	2018.03.0.20230918.0	62,3 MB	Solo `x86-64`
Amazon Linux 2	2,0,20230926,0	64,2 MB	`aarch64` è di 1,6 MB più grande di `x86-64`
Immagine di container di base Amazon Linux 2023	20232,20231002,0	52,4 MB	
Immagine di container minima Amazon Linux 2023	2023.2.20231002.0-minimal	35,2 MB	

Uso dell'immagine di container minima AL2023

L'immagine del contenitore minimo AL2023 è disponibile su ECR e il `2023-minimal` tag punterà sempre all'immagine del contenitore minimo più recente basata su AL2023, mentre il `minimal` tag può essere aggiornato a una versione di Amazon Linux più recente di AL2023.

Puoi estrarre questi tag usando `docker` il seguente esempio:

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:minimal
```

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023-minimal
```

L'esempio seguente mostra un file `Dockerfile` che prende l'immagine minima del contenitore e installa GCC su di essa:

```
FROM public.ecr.aws/amazonlinux/amazonlinux:2023-minimal
RUN dnf install -y gcc && dnf clean all
```

Creazione di immagini minime di contenitori AL2023

L'immagine del contenitore AL2023 è costruita con gli stessi componenti software inclusi nell'AMI AL2023. Include un software che consente al livello di contenitore di base di comportarsi in modo simile all'esecuzione su un'istanza Amazon EC2, ad esempio il gestore di pacchetti. `dnf` Questa sezione spiega come costruire da zero un contenitore che includa solo le dipendenze minime necessarie per un'applicazione.

> **Note**
>
> Le immagini standard del contenitore AL2023 sono adatte alla maggior parte dei casi d'uso. L'uso dell'immagine di container standard semplifica la creazione sulla base dell'immagine. Un'immagine contenitore semplice rende più difficile la creazione sulla base dell'immagine.

Per creare un container con dipendenze minime essenziali per un'applicazione

1. Determina le dipendenze di runtime. Questo aspetto varia a seconda dell'applicazione.
2. Crea un `Dockerfile`/`Containerfile` che consenta di sviluppare `FROM scratch`. Il seguente esempio di `Dockerfile` può essere usato per creare un container che include solo la shell `bash` e le relative dipendenze.

   ```
   FROM public.ecr.aws/amazonlinux/amazonlinux:2023 as build
   RUN mkdir /sysroot
   RUN dnf --releasever=$(rpm -q system-release --qf '%{VERSION}') \
     --installroot /sysroot \
     -y \
     --setopt=install_weak_deps=False \
   ```

```
  install bash

FROM scratch
COPY --from=build /sysroot /
WORKDIR /
ENTRYPOINT ["/bin/bash"]
```

- Questo `Dockerfile` funziona tramite:

  1. Avvio di un container AL2023 denominato `build`. Questo container viene utilizzato per il bootstrap dei container essenziali; non viene implementato, ma genera il container da implementare.
  2. Creazione della directory `/sysroot`. In questa directory il container `build` installa le dipendenze necessarie per il container essenziale. In un passaggio successivo, il percorso `/sysroot` viene impacchettato per diventare la directory principale dell'immagine essenziale.

     Usando l'opzione `--installroot` per `dnf` in questo modo permette di creare le altre immagini AL2023. Si tratta di una funzionalità di `dnf` che consente il funzionamento dei programmi di installazione e degli strumenti per la creazione di immagini.
  3. Richiamo di `dnf` per installare pacchetti in `/sysroot`.

     Il comando `rpm -q system-release --qf '%{VERSION}'` interroga (`-q`) il pacchetto `system-release`, impostando il formato della query (`--qf`) per stampare la versione del pacchetto sottoposta a query (la variabile `%{VERSION}` è la variabile `rpm` per la versione di `RPM`).

     Impostando l'argomento `--releasever` di `dnf` sulla versione di `system-release` nel container `build`, il `Dockerfile` può essere utilizzato per creare nuovamente il container essenziali ogni volta che viene rilasciata un'immagine di container di base aggiornata di Amazon Linux.

     È possibile impostarlo su qualsiasi versione di Amazon Linux 2023, `--releasever` ad esempio 2023.3.20240219. Ciò significherebbe che il `build` contenitore funzionerebbe come l'ultima versione AL2023, ma creerebbe il contenitore barebones a partire dalla versione 2023.3.20240219 indipendentemente dalla versione corrente di AL2023.

L'opzione di configurazione `--setopt=install_weak_deps=False` istruisce `dnf` affinché installi solo le dipendenze che sono richieste, anziché quelle consigliate o suggerite.

4. Copia del sistema installato nella directory principale di un container vuoto (`FROM scratch`).
5. Impostazione di `ENTRYPOINT` come binario desiderato, in questo caso `/bin/bash`.

3. Crea una directory vuota e aggiungi il contenuto dell'esempio riportato nel passaggio 2 a un file denominato `Dockerfile`.

```
$ mkdir al2023-barebones-bash-example
 $ cd al2023-barebones-bash-example
 $ cat > Dockerfile <<EOF
FROM public.ecr.aws/amazonlinux/amazonlinux:2023 as build
RUN mkdir /sysroot
RUN dnf --releasever=$(rpm -q system-release --qf '%{VERSION}') \
  --installroot /sysroot \
  -y \
  --setopt=install_weak_deps=False \
  install bash && dnf --installroot /sysroot clean all

FROM scratch
COPY --from=build /sysroot /
WORKDIR /
ENTRYPOINT ["/bin/bash"]
EOF
```

4. Crea il container eseguendo il comando seguente.

```
$ docker build -t al2023-barebones-bash-example
```

5. Esegui il container usando il comando seguente per capire quanto è minimo un container solo `bash`.

```
$ docker run -it --rm al2023-barebones-bash-example
bash-5.2# rpm
bash: rpm: command not found
bash-5.2# du -sh /usr/
bash: du: command not found
bash-5.2# ls
```

```
bash: ls: command not found
bash-5.2# echo /bin/*
/bin/alias /bin/bash /bin/bashbug /bin/bashbug-64 /bin/bg /bin/catchsegv /bin/cd /
bin/command /bin/fc /bin/fg /bin/gencat /bin/getconf /bin/getent /bin/getopts /
bin/hash /bin/iconv /bin/jobs /bin/ld.so /bin/ldd /bin/locale /bin/localedef /
bin/pldd /bin/read /bin/sh /bin/sotruss /bin/sprof /bin/type /bin/tzselect /bin/
ulimit /bin/umask /bin/unalias /bin/wait /bin/zdump
```

Per un esempio più pratico, la procedura seguente consente di creare un container per un'applicazione C che visualizza `Hello World!`.

1. Crea una directory vuota, quindi aggiungi il codice sorgente C e `Dockerfile`.

```
$ mkdir al2023-barebones-c-hello-world-example
$ cd al2023-barebones-c-hello-world-example
$ cat > hello-world.c <<EOF
#include <stdio.h>
int main(void)
{
  printf("Hello World!\n");
  return 0;
}
EOF

$ cat > Dockerfile <<EOF
FROM public.ecr.aws/amazonlinux/amazonlinux:2023 as build
COPY hello-world.c /
RUN dnf -y install gcc
RUN gcc -o hello-world hello-world.c
RUN mkdir /sysroot
RUN mv hello-world /sysroot/
RUN dnf --releasever=$(rpm -q system-release --qf '%{VERSION}') \
  --installroot /sysroot \
  -y \
  --setopt=install_weak_deps=False \
  install glibc && dnf --installroot /sysroot clean all

FROM scratch
COPY --from=build /sysroot /
WORKDIR /
ENTRYPOINT ["/hello-world"]
EOF
```

2. Avvia il container utilizzando il comando seguente.

```
$ docker build -t al2023-barebones-c-hello-world-example .
```

3. Esegui il container utilizzando il comando seguente.

```
$ docker run -it --rm al2023-barebones-c-hello-world-example
Hello World!
```

Confronto dei pacchetti installati sulle immagini di container Amazon Linux 2023

Un confronto tra gli RPM presenti nell'immagine del contenitore di base AL2023 rispetto agli RPM presenti nell'immagine minima del contenitore AL2023.

Pacchetto	Container	Contenitore minimo
alternatives	1.15	1.15
amazon-linux-repo-cdn	2023,420240319	2023,420240319
audit-libs	3,0,6	30.6
basesystem	11	11
bash	5,2,15	5,2,15
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023,2,64	2023,2,64
coreutils-single	8,32	8,32
crypto-policies	20220428	20220428
curl-minimal	8,5,0	8,5,0

Pacchetto	Container	Contenitore minimo
dnf	4.14.0	
dnf-data	4.14.0	4.14.0
elfutils-default-yama-scope	0.188	
elfutils-libelf	0.188	
elfutils-libs	0.188	
expat	2.5.0	
file-libs	5,39	5,39
filesystem	3,14	3,14
gawk	5.1.0	5.1.0
gdbm-libs	1,19	
glib2	2,74,7	2,74,7
glibc	2,34	2,34
glibc-common	2,34	2,34
glibc-minimal-langpack	2,34	2,34
gmp	62,1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gobject-introspection		1,73,0
gpgme	1.15.1	1.15.1
grep	3.8	3.8
json-c	0,14	0,14

Pacchetto	Container	Contenitore minimo
keyutils-libs	1.6.3	1.6.3
krb5-libs	1,21	1,21
libacl	2.3.1	2.3.1
libarchive	3,5,3	3,5,3
libassuan	2,5,5	2,5,5
libattr	2.5.1	2.5.1
libblkid	2,37,4	2,37,4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2
libcom_err	1,446,5	1,46,5
libcomps	01,20	
libcurl-minimal	8,5,0	8,5,0
libdnf	0,69,0	0,69,0
libffi	34.4	34.4
libgcc	114,1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	
libgpg-error	1,42	1,42
libidn2	2.3.2	2.3.2
libmodulemd	2.13.0	2.13.0

Pacchetto	Container	Contenitore minimo
libmount	2,37,4	2,37,4
libnghttp2	1,57,0	1,57,0
libpeas		1.32.0
libpsl	0,21,1	0,21,1
librepo	1,14,5	1,14,5
libreport-filesystem	2,15,2	2,15,2
libselinux	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2,13	2,13
libsmartcols	2,37,4	2,37,4
libsolv	0,7,22	0,7,22
libstdc++	11,4,1	11.4.1
libtasn1	4,19,0	4,19,0
libunistring	0,9,10	0,9,10
libuuid	2,37,4	2,37,4
libverto	0,32	0,32
libxcrypt	4,4,33	
libxml2	2,10,4	210.4
libyaml	02,5	02,5
libzstd	1,5,5	1,5,5

Pacchetto	Container	Contenitore minimo
lua-libs	5.4.4	5.4.4
lz4-libs	1.9.4	1.9.4
microdnf		38,1
microdnf-dnf		38.1
mpfr	4.1.0	4.1.0
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
npth	1.6	1.6
openssl-libs	30,8	30,8
p11-kit	0,24,1	0,24,1
p11-kit-trust	0,24,1	0,24,1
pcre2	10,40	10,40
pcre2-syntax	10,40	10,40
popt	1,18	1,18
publicsuffix-list-dafsa	20240212	20240212
python3	3,9,16	
python3-dnf	4.14.0	
python3-gpg	1.15.1	
python3-hawkey	0,69,0	
python3-libcomps	01,20	

Pacchetto	Container	Contenitore minimo
python3-libdnf	0,69,0	
python3-libs	3,9,16	
python3-pip-wheel	21,31	
python3-rpm	4,16,1,3	
python3-setuptools-wheel	59,60	
readline	8.1	8.1
rpm	4,161,3	4,161,3
rpm-build-libs	4,161,3	
rpm-libs	4,161,3	4,161,3
rpm-sign-libs	4,161,3	
sed	4.8	4.8
setup	2,13,7	2,13,7
sqlite-libs	3,4,0	3,4,0
system-release	2023,420240319	2023,420240319
tzdata	2024a	
xz-libs	5.2.5	5.2.5
yum	4.14.0	
zlib	1,2,11	1,2,11

Confronto dei pacchetti installati sulle immagini di container e AMI minime Amazon Linux 2023

Un confronto tra gli RPM presenti sull'AMI minima AL2023 con gli RPM presenti sulla base AL2023 e sulle immagini minime del contenitore.

Pacchetto	AMI minima	Container	Contenitore minimo
alternatives	1.15	1.15	1.15
amazon-chrony-config	4.3		
amazon-ec2-net-utils	2.4.1		
amazon-linux-repo-cdn		2023,420240319	2023,420240319
amazon-linux-repo-s3	2023,420240319		
amazon-linux-sb-keys	2023,1		
audit	30.6		
audit-libs	30.6	30.6	30.6
awscli-2	2.14.5		
basesystem	11	11	11
bash	5,2,15	5,2,15	5,2,15
bzip2-libs	1.0.8	1.0.8	1.0.8
ca-certificates	2023,2,64	2023,2,64	2023,2,64
checkpolicy	3.4		
chrony	4.3		
cloud-init	222,2		

Pacchetto	AMI minima	Container	Contenitore minimo
cloud-init-cfg-ec2	222,2		
cloud-utils-growpart	0,31		
coreutils	8,32		
coreutils-common	8,32		
coreutils-single		8,32	8,32
cpio	2,13		
cracklib	2,9,6		
cracklib-dicts	29.6		
crypto-policies	20220428	20220428	20220428
cryptsetup-libs	2.6.1		
curl-minimal	8,5,0	8,5,0	8,5,0
cyrus-sasl-lib	2,1,27		
dbus	1,12,28		
dbus-broker	32		
dbus-common	1,12,28		
dbus-libs	1,12,28		
device-mapper	1,02,185		
device-mapper-libs	1,02,185		
diffutils	3.8		
dnf	4.14.0	4.14.0	

Pacchetto	AMI minima	Container	Contenitore minimo
dnf-data	4.14.0	4.14.0	4.14.0
dnf-plugin-release-notification	1.2		
dnf-plugin-support-info	1.2		
dnf-plugins-core	4.3.0		
dracut	055		
dracut-config-ec2	3.0		
dracut-config-generic	055		
e2fsprogs	1,446,5		
e2fsprogs-libs	1,46,5		
ec2-utils	2.2.0		
efi-filesystem	5		
efivar	38		
efivar-libs	38		
elfutils-default-yama-scope	0.188	0.188	
elfutils-libelf	0.188	0.188	
elfutils-libs	0.188	0.188	
expat	2.5.0	2.5.0	
file	5,39		
file-libs	5,39	5,39	5,39

Pacchetto	AMI minima	Container	Contenitore minimo
filesystem	3,14	3,14	3,14
findutils	4.8.0		
fuse-libs	2,9,9		
gawk	5.1.0	5.1.0	5.1.0
gdbm-libs	1,19	1,19	
gdisk	1.0.8		
gettext	0,21		
gettext-libs	0,21		
glib2	2,74,7	2,74,7	2,74,7
glibc	2,34	2,34	2,34
glibc-all-langpacks	2,34		
glibc-common	2,34	2,34	2,34
glibc-locale-source	2,34		
glibc-minimal-lang pack		2,34	2,34
gmp	62,1	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7	2.3.7
gnutls	3.8.0		
gobject-introspection			1,73,0
gpgme	1.15.1	1.15.1	1.15.1
grep	3.8	3.8	3.8

Pacchetto	AMI minima	Container	Contenitore minimo
groff-base	1,22,4		
grub2-common	2,06		
grub2-efi-aa64-ec2	2,06 (aarch64)		
grub2-efi-x64-ec2	2,06 (x86_64)		
grub2-pc-modules	2,06		
grub2-tools	2,06		
grub2-tools-minimal	2,06		
grubby	8,40		
gzip	1.12		
hostname	3,23		
hwdata	0,3353		
inih	49		
initscripts	10,09		
iproute	5.10.0		
iputils	20210202		
irqbalance	1.9.0		
jansson	2.14		
jitterentropy	3.4.1		
jq	1.7.1		
json-c	0,14	0,14	0,14

Pacchetto	AMI minima	Container	Contenitore minimo
kbd	2.4.0		
kbd-misc	2.4.0		
kernel	61,79		
kernel-livepatch-repo-s3	2023,420240319		
keyutils-libs	1.6.3	1.6.3	1.6.3
kmod	29		
kmod-libs	29		
krb5-libs	1,21	1,21	1,21
less	608		
libacl	2.3.1	2.3.1	2.3.1
libarchive	3,5,3	3,5,3	3,5,3
libargon2	20171227		
libassuan	2,5,5	2,5,5	2,5,5
libattr	2.5.1	2.5.1	2.5.1
libblkid	2,37,4	2,37,4	2,37,4
libcap	2,48	2,48	2,48
libcap-ng	0.8.2	0.8.2	0.8.2
libcbor	0.7.0		
libcom_err	1,446,5	1,46,5	1,46,5
libcomps	01,20	01,20	

Pacchetto	AMI minima	Container	Contenitore minimo
libcurl-minimal	8,5,0	8,5,0	8,5,0
libdb	5,3,28		
libdnf	0,69,0	0,69,0	0,69,0
libeconf	0,40		
libedit	3.1		
libfdisk	2,37,4		
libffi	34.4	34.4	34.4
libfido2	1.10.0		
libgcc	114,1	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2	1.10.2
libgomp	11.4.1	11.4.1	
libgpg-error	1,42	1,42	1,42
libidn2	2.3.2	2.3.2	2.3.2
libkcapi	1.4.0		
libkcapi-hmaccalc	1.4.0		
libmnl	1.0.4		
libmodulemd	2.13.0	2.13.0	2.13.0
libmount	2,37,4	2,37,4	2,37,4
libnghttp2	1,57,0	1,57,0	1,57,0
libpeas			1.32.0

Pacchetto	AMI minima	Container	Contenitore minimo
libpipeline	1.5.3		
libpsl	0,21,1	0,21,1	0,21,1
libpwquality	1.4.4		
librepo	1,14,5	1,14,5	1,14,5
libreport-filesystem	2,15,2	2,15,2	2,15,2
libseccomp	2.5.3		
libselinux	3.4	3.4	3.4
libselinux-utils	3.4		
libsemanage	3.4		
libsepol	3.4	3.4	3.4
libsigsegv	2,13	2,13	2,13
libsmartcols	2,37,4	2,37,4	2,37,4
libsolv	0,7,22	0,7,22	0,7,22
libss	1,446,5		
libstdc++	11.4.1	11.4.1	11.4.1
libtasn1	4,19,0	4,19,0	4,19,0
libtextstyle	0,21		
libunistring	0,9,10	0,9,10	0,9,10
libuser	0,63		
libutempter	1.2.1		

Pacchetto	AMI minima	Container	Contenitore minimo
libuuid	2,37,4	2,37,4	2,37,4
libverto	0,32	0,32	0,32
libxcrypt	4,4,33	4,4,33	
libxml2	2,10,4	210.4	210.4
libyaml	02,5	02,5	02,5
libzstd	1,5,5	1,5,5	1,5,5
logrotate	3,20,1		
lua-libs	5.4.4	5.4.4	5.4.4
lz4-libs	1.9.4	1.9.4	1.9.4
man-db	2,9,3		
microcode_ctl	2.1 (x86_64)		
microdnf			3.8.1
microdnf-dnf			38.1
mpfr	4.1.0	4.1.0	4.1.0
ncurses	6.2		
ncurses-base	6.2	6.2	6.2
ncurses-libs	6.2	6.2	6.2
net-tools	2.0		
nettle	3.8		
npth	1.6	1.6	1.6

Pacchetto	AMI minima	Container	Contenitore minimo
numactl-libs	2.0,14		
oniguruma	6,9,7,1		
openldap	2,4,57		
openssh	8.7p1		
openssh-clients	8,7p1		
openssh-server	8,7p1		
openssl	3,0,8		
openssl-libs	30,8	30,8	30,8
openssl-pkcs11	0,4,12		
os-prober	1,77		
p11-kit	0,24,1	0,24,1	0,24,1
p11-kit-trust	0,24,1	0,24,1	0,24,1
pam	1.5.1		
passwd	0,80		
pciutils	3.7.0		
pciutils-libs	3.7.0		
pcre2	10,40	10,40	10,40
pcre2-syntax	10,40	10,40	10,40
policycoreutils	3.4		
popt	1,18	1,18	1,18

Pacchetto	AMI minima	Container	Contenitore minimo
procps-ng	3,3,17		
psmisc	23,4		
publicsuffix-list-dafsa	20240212	20240212	20240212
python3	3,9,16	3,9,16	
python3-attrs	20,3,0		
python3-audit	30.6		
python3-awscrt	0,19,19		
python3-babel	2,9,1		
python3-cffi	1,14,5		
python3-chardet	4.0.0		
python3-colorama	04.4		
python3-configobj	50.6		
python3-cryptography	36,0		
python3-dateutil	28.1		
python3-dbus	1,2,18		
python3-distro	1.5.0		
python3-dnf	4.14.0	4.14.0	
python 3- dnf-plugins-core	4.3.0		
python3-docutils	0,16		
python3-gpg	1.15.1	1.15.1	

Pacchetto	AMI minima	Container	Contenitore minimo
python3-hawkey	0,69,0	0,69,0	
python3-idna	(2.10)		
python3-jinja2	211,3		
python3-jmespath	0.10.0		
python3-jsonpatch	1,21		
python3-jsonpointer	2.0		
python3-jsonschema	3.2.0		
python3-libcomps	01,20	01,20	
python3-libdnf	0,69,0	0,69,0	
python3-libs	3,9,16	3,9,16	
python3-libselinux	3.4		
python3-libsemanage	3.4		
python3-markupsafe	1.1.1		
python3-netifaces	0,10,6		
python3-oauthlib	3.0.2		
python3-pip-wheel	21,31	21,31	
python3-ply	3,11		
python3-policycore utils	3.4		
python3-prettytable	0.7.2		
python3-prompt-toolkit	3,0,24		

Pacchetto	AMI minima	Container	Contenitore minimo
python3-pycparser	2,20		
python3-pyrsistent	0,17,3		
python3-pyserial	3.4		
python3-pysocks	1.7.1		
python3-pytz	2022,7,1		
python3-pyyaml	5.4.1		
python3-requests	2,25,1		
python3-rpm	4,161,3	4,161,3	
python3-ruamel-yaml	0,16,6		
pitone 3- ruamel-ya ml-clib	0.1.2		
python3-setools	4.4.1		
python3-setuptools	59,6,0		
python3-setuptools-wheel	59,6,0	59,6,0	
python3-six	1.15.0		
sistema python3	235		
python3-urllib3	1,25,10		
python3-wcwidth	0,2,5		
readline	8.1	8.1	8.1
rng-tools	6,14		

Pacchetto	AMI minima	Container	Contenitore minimo
rootfiles	8.1		
rpm	4,16,13	4,161,3	4,161,3
rpm-build-libs	4,161,3	4,161,3	
rpm-libs	4,161,3	4,161,3	4,161,3
rpm-plugin-selinux	4,161,3		
rpm-plugin-systemd-inhibit	4,161,3		
rpm-sign-libs	4,161,3	4,161,3	
sbsigntools	0.9.4		
sed	4.8	4.8	4.8
selinux-policy	37,22		
selinux-policy-targeted	37,22		
setup	2,13,7	2,13,7	2,13,7
shadow-utils	4.9		
sqlite-libs	3,4,0	3,4,0	3,4,0
sudo	1,9,14		
sysctl-defaults	1		
system-release	2023,420240319	2023,420240319	2023,420240319
systemd	252,16		
systemd-libs	252,16		

Pacchetto	AMI minima	Container	Contenitore minimo
systemd-networkd	252,16		
systemd-pam	252,16		
systemd-resolved	252,16		
systemd-udev	252,16		
tar	1,34		
tzdata	2024a	2024a	
update-motd	2.2		
userspace-rcu	0.12.1		
util-linux	2,37,4		
util-linux-core	2,37,4		
vim-data	9,0,2153		
vim-minimal	9,0,2153		
which	2,21		
xfsprogs	5,18,0		
xz	5.2.5		
xz-libs	5.2.5	5.2.5	5.2.5
yum	4.14.0	4.14.0	
zlib	1,2,11	1,2,11	1,2,11
zram-generator	1.1.2		
zram-generator-defaults	1.1.2		

Pacchetto	AMI minima	Container	Contenitore minimo
zstd	1,5,5		

AL2023 su AWS Elastic Beanstalk

AWS Elastic Beanstalk è un servizio per l'implementazione e la scalabilità di applicazioni e servizi Web. Carica il codice ed Elastic Beanstalk gestirà automaticamente l'implementazione, dal provisioning della capacità, il sistema di bilanciamento del carico e il dimensionamento automatico, al monitoraggio dello stato delle applicazioni. Per ulteriori informazioni, consulta AWS Elastic Beanstalk.

Per usare Elastic Beanstalk, devi creare un'applicazione, caricare una versione dell'applicazione sotto forma di un bundle di origine dell'applicazione (ad esempio un file .war Java) in Elastic Beanstalk e fornire alcune informazioni sull'applicazione. Elastic Beanstalk avvia automaticamente un ambiente e crea e AWS configura le risorse necessarie per eseguire il codice. Per ulteriori informazioni, consulta la Guida per gli sviluppatori di AWS Elastic Beanstalk.

Le piattaforme Elastic Beanstalk Linux utilizzano le istanze Amazon EC2 e queste istanze eseguono Amazon Linux. A partire dal 4 agosto 2023, Elastic Beanstalk offre le seguenti ramificazioni della piattaforma basati su Amazon Linux 2023:Docker,Tomcat,Java SE,Node.js,PHP e Python. Elastic Beanstalk sta lavorando per rilasciare il supporto per AL2023 su altre piattaforme Elastic Beanstalk.

L'elenco completo del supporto delle piattaforme Elastic Beanstalk e delle piattaforme attuali basate su AL2023 è disponibile nella sezione Piattaforme Elastic Beanstalk Linux della Guida per gli sviluppatori di Elastic Beanstalk.

Puoi trovare le note di rilascio per le nuove piattaforme Elastic Beanstalk e le versioni delle piattaforme esistenti nelle note di rilascio di Elastic Beanstalk.

Utilizzo di AL2023 in AWS CloudShell

AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. AWS Management ConsoleÈ possibile accedere CloudShell da diversi modi AWS Management Console . Per ulteriori informazioni, vedi Come iniziare AWS CloudShell?

AWS CloudShell, che attualmente è basato su Amazon Linux 2, migrerà verso AL2023. La migrazione verso AL2023 inizierà a essere implementata ovunque a Regioni AWS partire dal 4

dicembre 2023. Per ulteriori informazioni sulla CloudShell migrazione ad AL2023, consulta AWS CloudShell Migrazione da Amazon Linux 2 ad Amazon Linux 2023.

Utilizzo di AMI Amazon ECS basate su AL2023 per ospitare carichi di lavoro containerizzati

> **Note**
>
> Per ulteriori informazioni su come utilizzare AL2023 all'interno di un container, consulta. AL2023 nei container

Amazon Elastic Container Service (Amazon ECS) è un servizio di orchestrazione di container completamente gestito che facilita l'implementazione, la gestione e il dimensionamento delle applicazioni containerizzate. Essendo un servizio completamente gestito, Amazon ECS include AWS configurazioni e best practice operative integrate. È integrato con strumenti AWS sia di terze parti, come Amazon Elastic Container Registry (Amazon ECR) e Docker. Questa integrazione consente ai team di concentrarsi più facilmente sulla creazione delle applicazioni piuttosto che sull'ambiente. Puoi eseguire e dimensionare i carichi di lavoro dei container nelle regioni AWS nel cloud, senza la complessità legata alla gestione di un piano di controllo (control-plane).

Puoi ospitare carichi di lavoro containerizzati su AL2023 utilizzando l'AMI ottimizzata per Amazon ECS basata su AL2023. Per ulteriori informazioni, consulta l'AMI ottimizzata per Amazon ECS

Modifiche in AL2023 per Amazon ECS rispetto a AL2

Come con AL2, AL2023 fornisce i pacchetti di base necessari per l'esecuzione come istanza Amazon ECS Linux. In AL2 i `ecs-init` pacchetti `containerd`docker, e erano disponibili tramite`amazon-linux-extras`, mentre AL2023 include questi pacchetti nei repository principali.

Con gli aggiornamenti deterministici tramite la funzionalità di repository con versioni, ogni AMI AL2023 per impostazione predefinita è bloccata su una versione di repository specifica. Questo vale anche per l'AMI ottimizzata per Amazon ECS AL2023. Tutti gli aggiornamenti dell'ambiente possono essere gestiti e testati con attenzione prima della distribuzione, oltre a fornire un modo semplice per ripristinare il contenuto di un'AMI precedente in caso di problemi. Per ulteriori informazioni su questa funzionalità di AL2023, consulta Utilizzo degli aggiornamenti deterministici tramite il repository con versioni su AL2023.

AL2023 passa a cgroup v2 tramite l'interfaccia cgroup v1 supportata in AL2. Per ulteriori informazioni, consulta Gerarchia dei gruppi di controllo unificati (cgroup v2).

> **Note**
>
> Le versioni AL2023 precedenti alla 2023.2.20230920 (la prima versione AL2023.2) contenevano un bug per la gestione di Out-of-Memory (OOM) all'interno di un cgroup. `systemd` Tutti i processi in cgroup venivano sempre interrotti invece che OOM-Killer scegliesse un processo alla volta, che è il comportamento previsto.
> Si trattava di una regressione rispetto al comportamento di AL2 ed è stata risolta a partire dalla versione 2023.2.20230920 di AL2023.

Il codice per creare l'AMI ottimizzata per Amazon ECS è disponibile nel amazon-ecs-ami GitHub progetto. Le note di rilascio descrivono quale versione AL2023 è mappata a quale versione AMI Amazon ECS.

Personalizzazione dell'AMI ottimizzata per Amazon ECS basata su AL2023

> **Important**
>
> Ti consigliamo di utilizzare l'AMI AL2023 ottimizzata per Amazon ECS. Per ulteriori informazioni, consulta l'AMI ottimizzata per Amazon ECS nella Amazon Elastic Container Service Developer Guide.

Puoi usare gli stessi script di build utilizzati da Amazon ECS per creare AMI personalizzate. Per ulteriori informazioni, consulta lo script di compilazione dell'AMI Linux ottimizzato per Amazon ECS.

Utilizzo di Amazon Elastic File System su AL2023

Amazon Elastic File System (Amazon EFS) fornisce un'archiviazione di file serverless e completamente elastica in modo da poter condividere i dati dei file senza dover fornire o gestire la capacità e le prestazioni di archiviazione. Amazon EFS è progettato per eseguire il dimensionamento on-demand fino a svariati petabyte senza interrompere le applicazioni, aumentando e riducendo automaticamente le dimensioni man mano che aggiungi e rimuovi i file. Poiché Amazon EFS dispone di una semplice interfaccia di servizi Web, è possibile creare e configurare i file system in modo rapido e semplice. Il servizio gestisce tutta l'infrastruttura di storage dei file per conto dell'utente, il che

significa che è possibile evitare attività complesse come la distribuzione, l'applicazione di patch e la manutenzione di complesse configurazioni di file system.

Amazon EFS supporta il protocollo Network File System versione 4 (NFSv4.1 e NFSv4.0). Pertanto, le applicazioni e gli strumenti attualmente in uso potranno continuare a funzionare correttamente con Amazon EFS. Più istanze di calcolo, tra cui Amazon EC2, Amazon ECS e AWS Lambda, possono accedere contemporaneamente a un file system Amazon EFS. Di conseguenza, un file system EFS può fornire un'origine dati comune per carichi di lavoro e applicazioni in esecuzione su più server o istanze di calcolo.

Installazione di **`amazon-efs-utils`** su AL2023

Il `amazon-efs-utils` pacchetto è disponibile nei repository AL2023 per essere installato e utilizzato per accedere ai file system Amazon EFS.

Installazione del pacchetto **`amazon-efs-utils`** su AL2023

- Installa `amazon-efs-utils` utilizzando il seguente comando.

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

Montaggio di un file system Amazon EFS su AL2023

Dopo `amazon-efs-utils` l'installazione, puoi montare un file system Amazon EFS sulla tua istanza AL2023.

Montaggio di un file system Amazon EFS su AL2023

- Per eseguire il montaggio utilizzando l'id del file system, usa il seguente comando.

```
sudo mount -t efs file-system-id efs-mount-point/
```

Puoi eseguire anche il montaggio del file system in modo che i dati in transito siano crittografati utilizzando TLS oppure il nome DNS o l'IP di destinazione di montaggio anziché l'id del file system. Per ulteriori informazioni, consulta la pagina dedicata al montaggio su istanze Amazon Linux utilizzando l'assistente per il montaggio EFS.

Utilizzo di Amazon EMR basato su AL2023

Amazon EMR è un servizio Web che rende più semplice ed efficiente l'elaborazione di grandi quantità di dati utilizzando Apache Hadoop e i servizi offerti da AWS.

Versioni Amazon EMR basate su AL2023

La versione 7.0.0 di Amazon EMR è stata la prima versione basata su AL2023. Con questa versione, AL2023 è il sistema operativo di base per Amazon EMR, che offre tutti i vantaggi di AL2023 ad Amazon EMR. Per ulteriori informazioni, consulta le note di rilascio di Amazon EMR 7.0.0.

AL2023 basato su Amazon EMR su EKS

Amazon EMR su EKS 6.13 è stato il primo rilascio a introdurre AL2023 come opzione. Con questo rilascio, puoi avviare Spark con AL2023 come sistema operativo, insieme al runtime Java 17. Per ulteriori informazioni, consulta le note di rilascio di Amazon EMR su EKS 6.13 e tutte le note di rilascio di Amazon EMR su EKS.

Utilizzo di AL2023 in AWS Lambda

Con AWS Lambda, puoi eseguire codice senza effettuare il provisioning o gestire server. Verrà addebitato soltanto il tempo di calcolo utilizzato e non verrà addebitato alcun costo quando il codice non è in esecuzione. Puoi eseguire codice per qualsiasi tipo di applicazione o servizio di back-end, senza alcuna amministrazione. Basta caricare il codice e Lambda penserà a tutto ciò che serve per eseguirlo e dimensionarlo con alta disponibilità.

Runtime **`provided.al2023`** gestito e immagine del contenitore AL2023

Il runtime di `provided.al2023` base si basa sull'immagine minima del contenitore AL2023 e fornisce un runtime gestito Lambda e un'immagine di base del contenitore basati su AL2023. Poiché il `provided.al2023` runtime si basa sull'immagine minima del contenitore AL2023, è sostanzialmente più piccolo (meno di 40 MB) rispetto al runtime di circa 109 MB. `provided.al2`

Per ulteriori informazioni, consulta Lambda runtimes e Working with Lambda container images.

Runtime Lambda basate su AL2023

Le versioni future dei runtime linguistici gestiti, come Node.js 20, Python 3.12, Java 21 e .NET 8, sono basate su AL2023 e verranno utilizzate `provided.al2023` come immagine di base come descritto nell'annuncio dei runtime basati su AL2023.

Funzioni Lambda basate su AL2023

- Funzioni Lambda AL2023 scritte in Go
- Funzioni Lambda AL2023 scritte in Rust

Per ulteriori informazioni, consulta Lambda runtimes nella Developer Guide.AWS Lambda

Tutorial

I seguenti tutorial mostrano come eseguire attività comuni utilizzando istanze Amazon EC2 che eseguono Amazon Linux 2023 (AL2023). Per i tutorial video, consulta Video didattici e laboratori. AWS

Per le istruzioni su AL2, consulta i tutorial per le istanze Amazon EC2 che eseguono Linux nella Amazon EC2 User Guide for Linux Instances.

Tutorial

- Tutorial: Installare un server LAMP su AL2023
- Tutorial: configurare SSL/TLS su AL2023
- Tutorial: Ospita un WordPress blog su AL2023

Tutorial: Installare un server LAMP su AL2023

Le seguenti procedure consentono di installare un server Web Apache con supporto PHP e MariaDB (un fork di MySQL sviluppato dalla comunità) sull'istanza AL2023 (a volte chiamata server web LAMP o stack LAMP). 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**
>
> Queste procedure sono destinate all'uso con AL2023. 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. Per Ubuntu, consulta la seguente documentazione della comunità Ubuntu: ApacheMySQLPHP. Per altre distribuzioni, consulta la relativa documentazione specifica.

Attività

- Fase 1: preparare il server LAMP
- Fase 2: verificare il server LAMP
- Fase 3: proteggere il server di database
- Fase 4: Installazione (facoltativa) phpMyAdmin

- Risoluzione dei problemi
- Argomenti correlati

Fase 1: preparare il server LAMP

Prerequisiti

- Questo tutorial presuppone che tu abbia già lanciato una nuova istanza utilizzando AL2023, con un nome DNS pubblico raggiungibile da Internet. Per ulteriori informazioni, consulta AL2023 su Amazon EC2. 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 Autorizza il traffico in entrata per le tue istanze Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.
- La seguente procedura installa l'ultima versione di PHP disponibile su AL2023, attualmente 8.1. Se hai in programma di utilizzare applicazioni PHP diverse da quelle descritte in questo tutorial, devi verificare che siano compatibili con la versione 8.1.

Per preparare il server LAMP

1. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connessione alle istanze AL2023.
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 accertarsi che siano disponibili gli aggiornamenti della sicurezza e le correzioni dei bug più recenti.

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

   ```
   [ec2-user ~]$ sudo dnf update -y
   ```
3. Installa le versioni più recenti del server web Apache e dei pacchetti PHP per AL2023.

   ```
   [ec2-user ~]$ sudo dnf install -y httpd wget php-fpm php-mysqli php-json php php-devel
   ```
4. Installa i pacchetti software MariaDB. Utilizzare il comando dnf install per installare contemporaneamente più pacchetti software e tutte le dipendenze correlate.

```
[ec2-user ~]$ sudo dnf install mariadb105-server
```

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

```
[ec2-user ~]$ sudo dnf info package_name
```

Esempio:

```
[root@ip-172-31-25-170 ec2-user]# dnf info mariadb105
Last metadata expiration check: 0:00:16 ago on Tue Feb 14 21:35:13 2023.
Installed Packages
Name         : mariadb105
Epoch        : 3
Version      : 10.5.16
Release      : 1.amzn2023.0.6
Architecture : x86_64
Size         : 18 M
Source       : mariadb105-10.5.16-1.amzn2023.0.6.src.rpm
Repository   : @System
From repo    : amazonlinux
Summary      : A very fast and robust SQL database server
URL          : http://mariadb.org
License      : GPLv2 and LGPLv2
Description  : MariaDB is a community developed fork from MySQL - a multi-user,
 multi-threaded
             : SQL database server. It is a client/server implementation consisting
 of
             : a server daemon (mariadbd) and many different client programs and
 libraries.
             : The base package contains the standard MariaDB/MySQL client programs
 and
             : utilities.
```

5. Avviare il server Web Apache.

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

6. 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
```

7. 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'avvio è stato creato un gruppo di sicurezza launch-wizard-***N*** per la tua istanza. Se non hai aggiunto regole del gruppo di sicurezza supplementari, questo gruppo contiene una singola regola per consentire connessioni SSH.

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

   b. Nel riquadro di navigazione sinistro, scegli Istanze e seleziona la tua 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'uso di `0.0.0.0/0` consente a tutti gli indirizzi IPv4 di accedere all'istanza tramite SSH. Questo è accettabile per un breve periodo di tempo in un ambiente di test, ma non è sicuro 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. Se non esiste alcuna regola in entrata per consentire connessioni HTTP (porta 80), la regola deve essere aggiunta ora. Scegliere il collegamento per il gruppo di sicurezza. Utilizzando le procedure descritte nella sezione Autorizzazione del traffico in entrata per le istanze Linux, 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

8. 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`, dovresti visualizzare la pagina di test di Apache che mostra il messaggio "Funziona!".

   Puoi ottenere il DNS pubblico per la tua istanza utilizzando la console Amazon EC2 (controlla la colonna DNS IPv4 pubblico; se questa colonna è nascosta, scegli Preferenze (l'icona a forma di ingranaggio) e attiva DNS IPv4 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 utilizzi Amazon Linux, potrebbe inoltre essere necessario anche configurare il firewall sulla tua istanza per consentire queste 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 `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 tramite un browser Web, gli URL visitati, il contenuto delle pagine Web ricevute e i contenuti (incluse le password) di tutti i moduli HTML inviati sono tutti visibili a persone non autorizzate in qualsiasi punto del 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: configurare SSL/TLS su AL2023.

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.

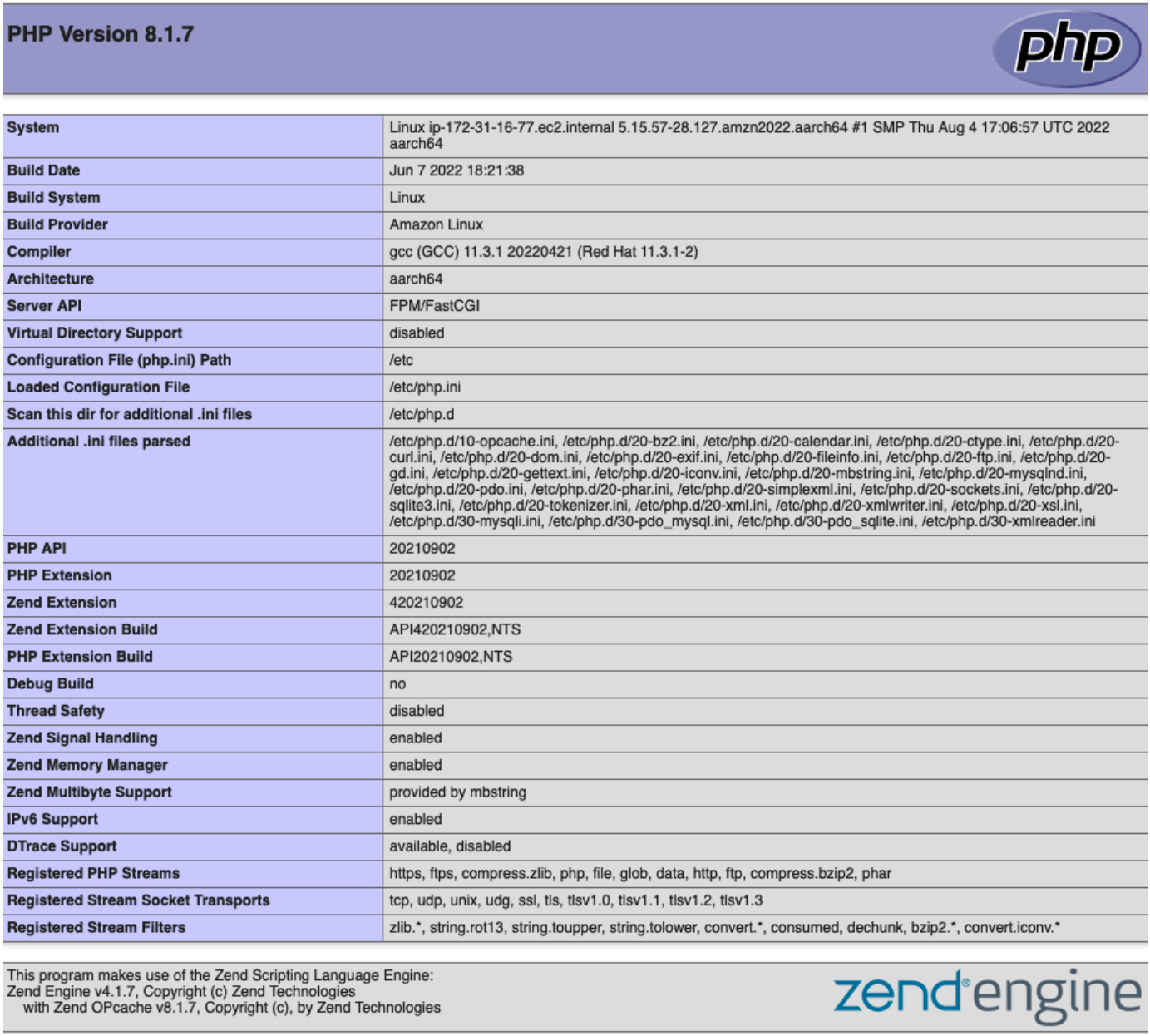
   ```
   [ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
   ```

   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 8.1.7

System	Linux ip-172-31-16-77.ec2.internal 5.15.57-28.127.amzn2022.aarch64 #1 SMP Thu Aug 4 17:06:57 UTC 2022 aarch64
Build Date	Jun 7 2022 18:21:38
Build System	Linux
Build Provider	Amazon Linux
Compiler	gcc (GCC) 11.3.1 20220421 (Red Hat 11.3.1-2)
Architecture	aarch64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,NTS
PHP Extension Build	API20210902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.1.7, Copyright (c) Zend Technologies
with Zend OPcache v8.1.7, Copyright (c), by Zend Technologies

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 dnf 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*.

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, visita la pagina 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: Installazione (facoltativa) 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 consigliamo di utilizzare `phpMyAdmin` per accedere a un server LAMP, a meno che non sia stato abilitato SSL/TLS in Apache; in caso contrario, la password dell'amministratore del database e altri dati vengono trasmessi in modo non sicuro tramite 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: configurare SSL/TLS su AL2023.

Per installare phpMyAdmin

1. Installare le dipendenze richieste.

```
[ec2-user ~]$ sudo dnf 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 file *`phpMyAdmintarball - latest-all-languages .tar.gz.`*

```
[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, digitate l'URL dell'installazione. phpMyAdmin Questo URL è l'indirizzo DNS pubblico (o indirizzo IP pubblico) dell'istanza seguito da una barra e dal nome della directory di installazione. Per 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, fate 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 possono verificarsi durante la configurazione di 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: configurare SSL/TLS su AL2023.
- 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 Autorizzare il traffico in entrata per le istanze Linux.

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 file sulla tua istanza Linux utilizzando WinSCP nella Guida per l'utente di Amazon EC2 per istanze Linux.
- Trasferisci file su istanze Linux utilizzando un client SCP nella Guida per l'utente di Amazon EC2 per istanze Linux.
- Tutorial: Ospita un WordPress blog su AL2023

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/

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: configurare SSL/TLS su AL2023

Il protocollo Secure Sockets Layer/Transport Layer Security (SSL/TLS) crea un canale crittografato tra un server Web e un client Web che protegge i dati in transito da eventuali intercettazioni. Questo tutorial spiega come aggiungere manualmente il supporto per SSL/TLS su un'istanza EC2 con AL2023 e 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. AL2023 disabilita il supporto lato server per tutte le versioni di SSL per impostazione predefinita. 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 in 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 AL2023. Se si sta tentando di impostare un'istanza EC2 che esegue una distribuzione diversa o un'istanza che esegue una versione precedente di Amazon Linux 2, alcune procedure in questa esercitazione potrebbero non funzionare. Per Ubuntu, consulta la documentazione seguente della community Ubuntu: Open SSL on 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, è possibile utilizzare AWS Certificate Manager (ACM) per AWS Nitro enclaves, un'applicazione enclave che permette di utilizzare certificati SSL/TLS pubblici e privati con le applicazioni Web e i server in esecuzione su istanze Amazon EC2 con AWS Nitro Enclaves. Nitro Enclaves è una funzionalità Amazon EC2 che consente la creazione di ambienti di calcolo isolati per proteggere ed elaborare in modo sicuro dati altamente sensibili, come certificati SSL/TLS e chiavi private.
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 AWSNitro Enclaves? e AWS Certificate Manager per Nitro Enclaves nella Guida per l'utente di AWS Nitro Enclaves.

Indice

Prerequisiti

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

- Avvia un'istanza AL2023 supportata da EBS. Per ulteriori informazioni, consulta AL2023 su Amazon EC2.
- 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 Autorizza il traffico in entrata per le tue istanze Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.
- Installare il server Web Apache. Per istruzioni, consulta. step-by-step Tutorial: Installare un server LAMP su AL2023 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

Questa procedura illustra il processo di configurazione di TLS su AL2023 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. Per ulteriori informazioni, consulta Connessione alle istanze AL2023.

   ```
   [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 dnf install openssl mod_ssl
   ```

3. Dopo aver inserito il seguente comando, verrà indirizzato a un prompt in cui è possibile immettere le informazioni sul sito.

```
[ec2-user ~]$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /
etc/pki/tls/private/apache-selfsigned.key -out /etc/pki/tls/certs/apache-
selfsigned.crt
```

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`

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. Questo sarà il file di certificato locale:

- `/etc/pki/tls/certs/localhost.crt`

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.

4. Riavviare Apache.

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

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

5. 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 CA considerate attendibili dal fornitore del browser ai fini di questa operazione. 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 al browser e questi lo verifica in base al relativo elenco di CA considerati attendibili. 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. Alcune CA forniscono certificati di livello base a titolo gratuito. La più importante è rappresentata dal 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 generata da OpenSSL in AL2023 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. Connettersi all'istanza e passare 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. Per ulteriori informazioni sulla connessione alla tua istanza, consulta Connessione alle istanze AL2023
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 tutte le CA forniscono lo stesso livello di supporto per elliptic-curve-based le chiavi RSA.

Verifica che la nuova chiave privata disponga di titolarità e autorizzazioni altamente restrittivi (owner=root, group=root, read/write solo per il proprietario). 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 (Nome località)	La località in cui si trova la tua organizza zione, ad esempio una città.	Seattle
Nome organizza zione	La denominazione legale completa della tua organizzazione. Non abbreviare il nome dell'organizzazione.	Example Corporation

Nome	Descrizione	Esempio
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`** . In un ambiente di testing con un certificato autofirmato e nessuna risoluzione DNS, il nome comune può essere composto solo dal nome host. Le CA offrono inoltre certificati più costosi, in grado di accettare nomi contenenti caratteri jolly, ad esempio **`*.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 questa fase, ti potrebbe venire

richiesto di fornire uno o più nomi alternativi di oggetto (SAN) 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 della CA lo consente, includi il nome comune nell'elenco di SAN. Alcuni CA lo 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, gruppo e autorizzazione del file corrispondano ai valori predefiniti altamente restrittivi di AL2023 (owner=root, group=root, read/write for owner only). 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, utilizzate i seguenti comandi per verificare che le impostazioni di proprietà, gruppo e autorizzazione dei file corrispondano ai valori predefiniti altamente restrittivi di AL2023 (owner=root, group=root, read/write for owner only).

```
[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**
>
> Alcune CA combinano il certificato host e i certificati intermedi in un unico file, rendendo inutile la direttiva `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 su AL2023 e con un certificato Certbot predefinito.

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:

✗ L'uso della crittografia RC4 è supportato su alcuni browser meno recenti. La crittografia rappresenta il nucleo matematico di un algoritmo di codifica. RC4, un tipo di crittografia rapida utilizzato per codificare i flussi di dati TLS, è noto per essere caratterizzato da diversi punti deboli gravi. 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 ulteriori informazioni, vedere l'utile risorsa sulla sicurezza/TLS lato server di Mozilla). 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 effetto secondario, queste crittografie 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.

Eseguendo nuovamente il test del dominio mediante il servizio Qualys SSL Labs, non dovrebbero più essere presenti né la vulnerabilità RC4 né gli altri avvisi e il riepilogo è 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 istanza EC2 AL2023 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 si esegue 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 esegue AL2023. Questo tutorial supporta solo le istanze appena create da un'AMI AL2023 ufficiale.

Tutorial: Ospita un WordPress blog su AL2023

Le seguenti procedure ti aiuteranno a installare, configurare e proteggere un WordPress blog sulla tua istanza AL2023. 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 AWS 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 preferisci ospitare il tuo WordPress blog su un'istanza Windows, consulta Implementare un WordPress blog sulla tua istanza Amazon EC2 Windows nella Amazon EC2 User Guide for Windows Instances. Se hai bisogno di una soluzione ad alta disponibilità con un database disaccoppiato, consulta la sezione Distribuzione di un sito Web ad alta disponibilità nella Developer Guide. WordPress AWS Elastic Beanstalk

> **Important**
>
> Queste procedure sono destinate all'uso con AL2023. Per 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

Ti consigliamo vivamente di associare un indirizzo IP elastico (EIP) all'istanza che stai utilizzando per ospitare un blog. WordPress 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, consultare Indirizzi IP elastici nella Guida per l'utente di Amazon EC2 per le istanze Linux. Il tutorial Tutorial: Installare un server LAMP su AL2023 include inoltre la procedura per configurare un gruppo di sicurezza che permetta 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.

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

Connect all'istanza e scarica il pacchetto WordPress di installazione. Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione alle istanze AL2023.

1. Scarica e installa questi pacchetti usando il comando seguente.

```
dnf install wget php-mysqlnd httpd php-fpm php-mysqli mariadb105-server php-json
 php php-devel -y
```

2. Puoi notare un avviso visualizzato con un messaggio simile nell'output (le versioni possono variare nel tempo):

```
WARNING:
```

```
  A newer release of "Amazon Linux" is available.

  Available Versions:

dnf update --releasever=2023.0.20230202

    Release notes:
     https://aws.amazon.com

  Version 2023.0.20230204:
    Run the following command to update to 2023.0.20230204:

      dnf update --releasever=2023.0.20230204 ... etc
```

Come best practice, consigliamo di mantenere il sistema operativo il più up-to-date possibile, ma potresti voler ripetere ogni versione per assicurarti che non vi siano conflitti nel tuo ambiente. Se l'installazione dei pacchetti precedenti indicati al passaggio 1 ha esito negativo, potrebbe essere necessario eseguire l'aggiornamento a una delle versioni più recenti elencate e riprovare.

3. Scaricate 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
```

4. 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. Avvia il server di database e il server Web.

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

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 Fase 3: proteggere il server di database (AL2023).

   ```
   [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. 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';
   ```

   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.

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. Visitare la pagina https://api.wordpress.org/secret-key/1.1/salt/ per generare in modo casuale una serie di valori di chiavi che è possibile copiare e incollare nel file `wp-config.php`. 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, vai a 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 service httpd stop. 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 AL2023

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 phpMyAdmin che installi potrebbe richiedere una versione minima specifica di questa libreria (ad esempio, la versione 8.1).

Usa il seguente comando per installare la libreria di disegni grafici PHP su AL2023. Ad esempio, se hai installato php8.1 dall'origine come parte dell'installazione dello stack LAMP, questo comando installa la versione 8.1 della libreria di disegni grafici PHP.

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

Per verificare la versione installata utilizza il seguente comando:

```
[ec2-user ~]$ sudo dnf list installed | grep php-gd
```

Di seguito è riportato un output di esempio:

```
php-gd.x86_64                  8.1.30-1.amzn2           @amazonlinux
```

Per installare la libreria di disegni grafici PHP nell'Amazon Linux AMI

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 phpMyAdmin che installi potrebbe richiedere una versione minima specifica di questa libreria (ad esempio, la versione 8.1).

Per verificare quali versioni sono disponibili utilizza il comando seguente:

```
[ec2-user ~]$ dnf list | grep php
```

Di seguito sono riportate righe di esempio dell'output per la libreria di disegni grafici PHP (versione 8.1):

```
php8.1.aarch64                                          8.1.7-1.amzn2023.0.1
                      @amazonlinux
php8.1-cli.aarch64                                      8.1.7-1.amzn2023.0.1
                      @amazonlinux
php8.1-common.aarch64                                   8.1.7-1.amzn2023.0.1
                      @amazonlinux
php8.1-devel.aarch64                                    8.1.7-1.amzn2023.0.1
                      @amazonlinux
php8.1-fpm.aarch64                                      8.1.7-1.amzn2023.0.1
                      @amazonlinux
php8.1-gd.aarch64                                       8.1.7-1.amzn2023.0.1
                      @amazonlinux
```

Utilizza il seguente comando per installare una versione specifica della libreria di disegni grafici PHP (ad esempio, versione php8.1) nell'AMI Amazon Linux:

```
[ec2-user ~]$ sudo dnf install -y php8.1-gd
```

Per correggere le autorizzazioni di file sul server Web Apache

Alcune delle funzionalità disponibili in Apache WordPress richiedono l'accesso in scrittura alla radice del documento Apache (come il caricamento di contenuti multimediali tramite le schermate di amministrazione). Se non già stato fatto, applicare le seguenti appartenenze e autorizzazioni di gruppo, come descritto con maggiore dettaglio in Tutorial: installa un server Web LAMP con Amazon Linux AMI.

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 intendi utilizzarlo anche WordPress come server FTP, qui avrai 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
```

Per eseguire lo script di WordPress installazione con AL2023

Sei pronto per l'installazione WordPress. I comandi utilizzati dipendono dal sistema operativo. I comandi di questa procedura sono destinati all'uso con AL2023. Usa la procedura che segue questa con AL2023 AMI.

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. Scegli WordPressInstalla per completare l'installazione. Per ulteriori informazioni, consulta Passaggio 5: Esecuzione dello script di installazione sul WordPress sito Web.

Per eseguire lo script WordPress di installazione con AL2023 AMI

1. Utilizzare il comando chkconfig per assicurarsi che i servizio `httpd` e di database vengano avviati a ogni avvio del sistema.

```
[ec2-user ~]$ sudo chkconfig httpd on && sudo chkconfig mariadb on
```

2. Verificare che il server di database sia in esecuzione.

```
[ec2-user ~]$ sudo service mariadb status
```

   Se il servizio di database non è in esecuzione, avviarlo.

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

3. Verificare che il server Web Apache (`httpd`) sia in esecuzione.

```
[ec2-user ~]$ sudo service httpd status
```

   Se il servizio `httpd` non è in esecuzione, avviarlo.

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

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. Scegli WordPressInstalla per completare l'installazione. Per ulteriori informazioni, consulta Passaggio 5: Esecuzione dello script di installazione sul WordPress sito Web.

Passaggi successivi

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 Crea la tua AMI nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Aumento della capacità

Se il tuo WordPress blog diventa popolare e hai bisogno di maggiore potenza di calcolo o spazio di archiviazione, considera i seguenti passaggi:

- Espandi lo spazio di storage sull'istanza. Per ulteriori informazioni, consulta Amazon EBS Elastic Volumes.
- 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 globale AWS per indirizzare il traffico verso un endpoint di applicazione integro nella regione AWS più vicino al client.

Scopri di più su WordPress

I seguenti collegamenti contengono ulteriori informazioni su WordPress.

- Per informazioni in merito WordPress, consultate la documentazione di aiuto del WordPress Codex disponibile su Codex.
- 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 https://wordpress.org/support/article//. changing-the-site-url

Se ciò si è verificato durante l' WordPress installazione, è 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 2023 al di fuori di Amazon EC2

Le immagini di container Amazon Linux 2023 possono essere eseguite in ambienti di runtime di container compatibili. Per ulteriori informazioni su come utilizzare Amazon Linux 2023 all'interno di un container, consultaAL2023 nei container.

Amazon Linux 2023 (AL2023) può essere eseguito anche come guest virtualizzato al di fuori dell'esecuzione diretta su Amazon EC2. Attualmente sono disponibili immagini KVM (`qcow2`), VMware (`OVA`) e Hyper-V (). `vhdx`

> **Note**
>
> La configurazione delle immagini di Amazon Linux 2023 è diversa da quella di Amazon Linux 2.
> Se in precedenza eseguivi Amazon Linux 2 come macchina virtuale on-premise, devi adattare la configurazione per renderla compatibile con AL2023.

Scarica le immagini di Amazon Linux 2023 da utilizzare con KVM, VMware e Hyper-V

Le immagini dei dischi di Amazon Linux 2023 da utilizzare con KVM, VMware e Hyper-V possono essere scaricate da cdn.amazonlinux.com.

Configurazioni supportate di Amazon Linux 2023 per l'uso in ambienti virtualizzati non Amazon EC2

Questa sezione descrive i requisiti per l'esecuzione di Amazon Linux 2023 in ambienti virtualizzati non Amazon EC2 come KVM, VMware o Hyper-V.

I Requisiti di sistema AL2023 di base si applica a tutti gli ambienti virtualizzati non Amazon EC2. Un elenco dettagliato dei modelli di dispositivi supportati è riportato per ogni ambiente hypervisor nei seguenti argomenti.

KVM, VMware e Hyper-V offrono molte opzioni di configurazione ed è necessario prestare attenzione per configurarle per le esigenze di sicurezza, prestazioni e affidabilità. Per ulteriori informazioni, consulta la documentazione fornita dall'hypervisor.

Argomenti

Requisiti per l'esecuzione di AL2023 su KVM

Questa sezione descrive i requisiti per l'esecuzione di AL2023 su KVM. Le immagini KVM di AL2023 sono disponibili per entrambe le architetture `aarch64` e `x86-64`. Questi requisiti si aggiungono alla base Requisiti di sistema AL2023 per le immagini KVM.

Argomenti

Requisiti dell'host KVM per l'esecuzione di AL2023 su KVM

Le immagini KVM sono attualmente qualificate su un host che esegue Ubuntu 22.04.3 LTS con la `qemu` versione6.2+dfsg-2ubuntu6.15, fornita da questa versione di Ubuntu, che utilizza un tipo di macchina. `q35`

Supporto del dispositivo per AL2023 su KVM

I modelli di dispositivi **`qemu`** testati per l'uso con immagini KVM AL2023 (sia **`aarch64`** e **`x86-64`**) sono:

- `virtio-blk` (dispositivo a blocchi `virtio`)
- `virtio-scsi` (controller SCSI `virtio` con dispositivo disco)
- `virtio-net` (dispositivo di rete `virtio`)
- `ahci` (da utilizzare con l'unità CD-ROM virtuale)
- `usb-storage` (superiore a `xhci`)

I modelli di **qemu** dispositivi aggiuntivi abilitati alla qualificazione delle immagini KVM AL2023, ma non utilizzati in modo intensivo, sono:

- VGA (qemu VGA) solo su `x86-64`
- `virtio-rng` (generatore virtuale di numeri casuali)
- Dispositivi tastiera AT e mouse PS/2 legacy
- Dispositivo seriale legacy

Modalità di avvio (UEFIeBIOS) supporto per AL2023 su KVM

L'immagine `x86-64` viene testata sia con entrambe le modalità di avvio legacy, BIOS e UEFI. Le immagini `aarch64` vengono testate con la modalità di avvio UEFI.

> **Note**
>
> Per impostazione predefinita, quando si utilizza la modalità di UEFI avvio, alcuni gestori di macchine virtuali forniranno alla macchina virtuale le chiavi Microsoft Secure Boot che abilitano Secure Boot. Questa configurazione non esegue l'avvio di AL2023.
> Poiché il boot loader AL2023 non è firmato da Microsoft, la macchina virtuale deve essere fornita senza chiavi UEFI o con le chiavi AL2023 per Secure Boot.

> **Important**
>
> Il supporto Secure Boot per le KVM immagini non è stato ancora convalidato.

Limitazioni all'esecuzione di AL2023 su KVM

Esistono alcune limitazioni note nell'esecuzione di AL2023 su KVM.

> **Note**
>
> Il codice che implementa alcune delle funzionalità non supportate elencate potrebbe esistere in AL2023 e funzionare correttamente. L'elenco delle funzionalità non supportate è disponibile in modo da consentirti di prendere decisioni informate su cosa fare affidamento oggi e su ciò che il team di Amazon Linux considererà funzionante nell'ambito dei futuri aggiornamenti.

Limitazioni note relative all'esecuzione di AL2023 su KVM

- L'agente guest KVM non è attualmente incluso nel pacchetto né supportato.
- Non sono supportati il collegamento e lo scollegamento a caldo di CPU, memoria o qualsiasi altro tipo di dispositivo.
- L'ibernazione delle VM non è supportata.
- La migrazione delle macchine virtuali non è supportata.
- Il passthrough di qualsiasi dispositivo, ad esempio PCI Passthrough o USB Passthrough, non è supportato.

Requisiti per l'esecuzione di AL2023 su VMware

Questa sezione descrive i requisiti per eseguire AL2023 su. VMware Le VMware immagini di AL2023 sono disponibili solo per l'`x86-64`architettura. VMwarele immagini per non `aarch64` sono disponibili o supportate. Questi requisiti si aggiungono alla base Requisiti di sistema AL2023 per le VMware immagini.

Argomenti

VMwarerequisiti dell'host per l'esecuzione di AL2023 su VMware

Le immagini VMware OVA AL2023 sono attualmente qualificate per quanto segue:

- VMwareWorkstation 17.5.0 in esecuzione su host che utilizzano un processore Intel (R) Xeon (R) Platinum 8124M
- VMwarevSphere 8.0 con un processore Intel (R) Xeon (R) Platinum 8275CL

Le immagini VMware OVA AL2023 specificano una versione hardware della macchina 13.

VMwareLa versione 13 dell'hardware della macchina è supportata da:

- ESXi 6.5 o versioni successive

- VMwareWorkstation 14 o versione successiva

Supporto del dispositivo per AL2023 su VMware

I seguenti modelli di VMware dispositivi sono stati testati per l'uso con immagini VMware OVA AL2023 (**`x86-64`**solo):

- `vmw_pvscsi`(controller VMware paravirtualizzatoSCSI)
- `vmxnet3`(dispositivo di rete paravirtualizzato) VMware
- `ata_piix` (IDE legacy da utilizzare solo con l'unità CD-ROM virtuale)

Modelli di VMware dispositivi aggiuntivi abilitati nella qualificazione delle VMware immagini AL2023, ma non utilizzati intensamente:

- `vmw_vmcie` relativa `vsock` interfaccia (trasporto tramite socket virtuale per l'VMwareagente guest)
- Dispositivo di memoria balloon `vmw_balloon`
- VMware`SVGA`controllore
- Dispositivi tastiera AT e mouse PS/2 legacy

Il pacchetto VMware guest agent (`open-vm-tools`) è disponibile e installato per impostazione predefinita nelle immagini VMware OVA AL2023.

Modalità di avvio (UEFIeBIOS) supporto per AL2023 su VMware

A partire dalla versione 2023.3.20231211, l'immagine VMware OVA AL2023 è stata convalidata sia in modalità legacy che in modalità di avvio. BIOS UEFI La configurazione predefinita di OVA è ancora obsoleta BIOS ma può essere modificata dall'utente.

> **Important**
>
> Richiede il supporto Secure BootUEFI, che non è stato convalidato per AL2023 in esecuzione. VMware

Limitazioni sull'esecuzione di AL2023 su VMware

Esistono alcune limitazioni note nell'esecuzione di AL2023 su. VMware

> **Note**
>
> Il codice che implementa alcune delle funzionalità non supportate elencate può esistere in AL2023 e funzionare correttamente. L'elenco delle funzionalità non supportate consente ai clienti di prendere decisioni informate su cosa poter utilizzare attualmente per lavorare, nonché su quello che il team di Amazon Linux renderà disponibile nell'ambito dei futuri aggiornamenti.

Limitazioni note relative all'esecuzione di AL2023 su VMware

- UEFISecure Boot non è attualmente convalidato con AL2023 attivo. VMware
- Non sono supportati il collegamento e lo scollegamento a caldo di CPU, memoria o qualsiasi altro tipo di dispositivo.
- L'ibernazione delle VM non è supportata.
- La migrazione delle macchine virtuali non è supportata.
- Il passthrough di qualsiasi dispositivo, ad esempio PCI Passthrough o USB Passthrough, non è supportato.

Requisiti per l'esecuzione di Amazon Linux 2023 su Hyper-V

Questa sezione descrive i requisiti per l'esecuzione di Amazon Linux 2023 su Hyper-V. Le immagini Hyper-V di AL2023 sono disponibili solo per l'architettura. `x86-64` Le immagini Hyper-V per non `aarch64` sono al momento disponibili o supportate.

Questa sezione descrive i requisiti aggiuntivi oltre alla base Requisiti di sistema AL2023 per le immagini Hyper-V.

Argomenti

- Requisiti dell'host Hyper-V per l'esecuzione di Amazon Linux 2023 su Hyper-V
- Supporto per dispositivi per Amazon Linux 2023 su Hyper-V
- Limitazioni all'esecuzione di Amazon Linux 2023 su Hyper-V

Requisiti dell'host Hyper-V per l'esecuzione di Amazon Linux 2023 su Hyper-V

La qualificazione principale di Amazon Linux 2023 su Hyper-V avviene su Windows Server 2022 in esecuzione su un'istanza EC2. `c5.metal`

Supporto per dispositivi per Amazon Linux 2023 su Hyper-V

Amazon Linux 2023 è testato su macchine virtuali Hyper-V di prima e seconda generazione con il seguente set di hardware virtualizzato:

- VM di prima generazione (avvio BIOS legacy)
- VM di seconda generazione (avvio UEFI - nessun avvio sicuro)
- I seguenti modelli di dispositivi sono testati per l'uso con immagini Hyper-V AL2023:
  - Storage virtuale Hyper-V *`hv_storvsc`* per il disco root e l'unità CD-ROM emulata su macchine virtuali di seconda generazione
  - IDE PIIX emulato per l'unità CD-ROM virtuale su macchine virtuali di *`ata_piix`* prima generazione
  - Ethernet virtuale Hyper-V `hv_netvsc`
- I seguenti modelli di dispositivi sono abilitati ma leggermente testati:
  - Modalità di testo VGA legacy su macchine virtuali di prima generazione
  - `simpledrmfb`Framebuffer basato su firmware UEFI su macchine virtuali di seconda generazione
  - Palloncino Hyper-V `hv_balloon`
  - Palloncino Hyper-V `hv_balloon`
  - Hyper-V HID/mouse `hid_hyperv`
- Le seguenti modalità del dispositivo non sono attualmente abilitate in AL2023:
  - Pass-through PCI Hyper-V
  - Grafica DRM Hyper-V

> **Important**
>
> Per le macchine virtuali di seconda generazione, Secure Boot non è supportato e deve essere disabilitato prima di avviare la macchina virtuale per avviare correttamente Amazon Linux 2023. Hyper-V attualmente supporta solo Secure Boot con componenti software firmati

con chiavi proprie di Microsoft, mentre il bootloader Amazon Linux è firmato da una chiave privata Amazon. Hyper-V non supporta l'importazione di chiavi di terze parti a questo punto.

Limitazioni all'esecuzione di Amazon Linux 2023 su Hyper-V

Di seguito sono riportate alcune limitazioni note nell'esecuzione di Amazon Linux 2023 su Hyper-V:

> **Note**
>
> Il codice che implementa alcune delle funzionalità non supportate elencate può esistere in AL2023 e funzionare correttamente. L'elenco delle funzionalità non supportate consente ai clienti di prendere decisioni informate su cosa poter utilizzare attualmente per lavorare, nonché su quello che il team di Amazon Linux renderà disponibile nell'ambito dei futuri aggiornamenti.

Limitazioni note relative all'esecuzione di AL2023 su Hyper-V

- La modalità UEFI Secure Boot non è attualmente supportata né funzionante con AL2023 su Hyper-V
- Non sono supportati il collegamento e lo scollegamento a caldo di CPU, memoria o qualsiasi altro tipo di dispositivo.
- L'ibernazione delle macchine virtuali (VM) non è supportata.
- La migrazione delle macchine virtuali (VM) non è supportata.
- Il passthrough di qualsiasi dispositivo, ad esempio PCI Passthrough o USB Passthrough, non è supportato.

Impostazione di Amazon Linux 2023 e configurazione di **`cloud-init`** in caso di utilizzato al di fuori di Amazon EC2

Questa sezione spiega come configurare una macchina virtuale Amazon Linux 2023 quando non viene eseguita direttamente su Amazon EC2, ad esempio su KVM, VMware o Hyper-V.

Per impostazione predefinita, le immagini di una macchina virtuale Amazon Linux 2023 non vengono fornite in provisioning con nessuna password utente o chiave ssh; ottengono la configurazione di

rete tramite DHCP sulla prima interfaccia di rete scoperta. Ciò significa che, senza configurazioni aggiuntive, non è possibile connettersi alla macchina virtuale risultante per impostazione predefinita.

Pertanto, è necessario fornire una qualche forma di configurazione per la macchina virtuale. Il meccanismo standard per eseguire questa operazione per Amazon Linux è tramite origini dati `cloud-init`.

Amazon Linux 2023 è stato qualificato con le seguenti origini dati:

NoCloud

Questo è il metodo tradizionale per configurare le immagini on-premise tramite un CD-ROM virtuale contenente un'immagine ISO9660 seed con file di configurazione `cloud-init`.

VMware

Amazon Linux 2023 supporta inoltre la configurazione di immagini VMware in esecuzione su vSphere tramite l'origine dati specifica di VMware tramite VMware `guestinfo.userdata` e `guestinfo.metadata`.

> **Note**
>
> La configurazione delle origini dati può essere diversa rispetto a quella di Amazon Linux 2. Più specificamente, Amazon Linux 2023 usa `systemd-networkd` per la sua configurazione e richiede l'uso di `cloud-init` "Configurazione di rete versione 2", come descritto nella documentazione sulla configurazione di rete di `cloud-init`.

La documentazione completa per i meccanismi di configurazione `cloud-init` per la versione di `cloud-init` pacchettizzata in Amazon Linux 2023 è disponibile nella documentazione sulla versione upstream di `cloud-init`.

NoCloud (`seed.iso`) `cloud-init` configurazione per Amazon Linux 2023 su KVM e VMware

Questa sezione spiega come creare e utilizzare un'`seed.iso`immagine per configurare Amazon Linux 2023 in esecuzione su KVM oVMware. Poiché KVM gli VMware ambienti non dispongono di Amazon EC2 Instance Meta Data Service (IMDS), è necessario un metodo alternativo per configurare Amazon Linux 2023 e fornire `seed.iso` un'immagine è uno di questi metodi.

L'immagine di avvio `seed.iso` include le informazioni di configurazione iniziale necessarie per avviare e configurare la nuova VM, ad esempio la configurazione di rete, il nome host e i dati utente.

> **Note**
>
> L'immagine `seed.iso` include solo le informazioni di configurazione richieste per avviare la VM. Non include invece i file del sistema operativo Amazon Linux 2023.

Per generare l'immagine `seed.iso`, sono necessari almeno due file di configurazione, talvolta tre:

`meta-data`

Questo file solitamente include il nome host per la macchina virtuale.

`user-data`

Questo file configura generalmente gli account utente e ne specifica le password, le coppie di chiavi ssh e/o i meccanismi di accesso. Per impostazione predefinita, le immagini KVM e VMware di Amazon Linux 2023 creano un account utente `ec2-user`. Puoi usare il file di configurazione `user-data` per impostare la password e/o le chiavi ssh per tale account utente predefinito.

`network-config` (facoltativo)

Questo file fornisce solitamente una configurazione di rete per la macchina virtuale che va a sostituire quella predefinita. La configurazione predefinita prevede l'uso di DHCP sulla prima interfaccia di rete disponibile.

Creazione dell'immagine disco **`seed.iso`**

1. Su un computer Linux o macOS, puoi creare una nuova cartella denominata `seedconfig` ed esplorarne il contenuto.

   > **Note**
   >
   > È possibile usare Windows o un altro sistema operativo per completare questi passaggi, ma è necessario trovare uno strumento equivalente a `mkisofs` per completare la creazione dell'immagine `seed.iso`.

2. Crea il file di configurazione `meta-data`.

a. Crea un nuovo file denominato `meta-data`.

b. Apri il file `meta-data` utilizzando l'editor preferito e aggiungi quanto segue, sostituendo *vm-hostname* con il nome host della VM:

```
local-hostname: vm-hostname
```

c. Salva e chiudi il file di configurazione `meta-data`.

3. Crea il file di configurazione `user-data`.

a. Crea un nuovo file denominato `user-data`.

b. Apri il file `user-data` utilizzando l'editor preferito e aggiungi quanto segue, effettuando le opportune sostituzioni:

```
#cloud-config
#vim:syntax=yaml
users:
# A user by the name 'ec2-user' is created in the image by default.
- default
- name: ec2-user
ssh_authorized_keys:
 - ssh-rsa ssh-key
# In the above line, replace ssh key with the content of your ssh public key.
```

c. Facoltativamente, puoi aggiungere altri account utente al file di configurazione. `user-data`

Puoi specificare account utente aggiuntivi, definendone i meccanismi di accesso, le password e le coppie di chiavi. Per ulteriori informazioni sulle direttive supportate, consulta la documentazione della versione upstream di `cloud-init`.

d. Salva e chiudi il file di configurazione `user-data`.

4. (Facoltativo) Crea il file di configurazione `network-config`.

a. Crea un nuovo file denominato `network-config`.

b. Apri il file `network-config` utilizzando l'editor preferito e aggiungi quanto segue, sostituendo i vari indirizzi IP con quelli appropriati per la configurazione desiderata.

```
version: 2
ethernets:
  enp1s0:
    addresses:
      - 192.168.122.161/24
    gateway4: 192.168.122.1
    nameservers:
      addresses: 192.168.122.1
```

> **Note**
>
> La configurazione di rete `cloud-init` fornisce meccanismi per la corrispondenza con l'indirizzo MAC dell'interfaccia anziché specificare il nome dell'interfaccia, che può cambiare a seconda della configurazione della VM. Queste (e altre) funzionalità `cloud-init` per la configurazione di rete sono descritte più dettagliatamente nella documentazione della versione 2 della configurazione di rete upstream `cloud-init`.

c. Salva e chiudi il file di configurazione `network-config`.

5. Crea l'immagine disco `seed.iso` utilizzando i file di configurazione `meta-data`, `user-data` e `network-config` opzionale che sono stati creati nei passaggi precedenti.

   Esegui una delle seguenti operazioni, a seconda del sistema operativo su stai creando l'immagine disco `seed.iso`.

   - Sui sistemi Linux, usa uno strumento come **`mkisofs`** o **`genisoimage`** per creare il file `seed.iso` completo. Vai alla cartella `seedconfig` ed esegui il comando seguente:

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

   - Se usi una `network-config`, includila nell'invocazione di **`mkisofs`**:

     ```
     $ mkisofs -output seed.iso -volid cidata -joliet -rock user-data meta-data
      network-config
     ```

   - Sui sistemi macOS, puoi usare uno strumento come **`hdiutil`** per generare il file `seed.iso` completo. Poiché **`hdiutil`** richiede un nome di percorso anziché un elenco di file, la stessa invocazione può essere utilizzata indipendentemente dal fatto che un file di configurazione `network-config` sia stato creato o meno.

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

6. Il file `seed.iso` risultante può ora essere collegato alla nuova macchina virtuale Amazon Linux 2023 tramite un'unità CD-ROM virtuale affinché `cloud-init` la trovi al primo avvio e applichi la configurazione al sistema.

VMware**`cloud-init`**configurazione guestinfo per AL2023 on VMware

VMwaregli ambienti non dispongono di Amazon EC2 Instance Meta Data Service (IMDS), quindi è necessario un metodo alternativo per configurare AL2023. Questa sezione descrive come utilizzare un meccanismo di configurazione alternativo all'unità CD-ROM `seed.iso` virtuale disponibile in VMware vSphere.

Questo metodo di configurazione utilizza il VMware `extraconfig` meccanismo per fornire i dati di configurazione a. `cloud-init` Per ciascuna delle seguenti chiavi, deve essere fornita una ***`keyname`*`.encoding`** proprietà corrispondente.

È possibile fornire al VMware `extraconfig` meccanismo le seguenti chiavi.

`guestinfo.metadata`

JSON o YAML contenenti metadati `cloud-init`

`guestinfo.userdata`

Un documento YAML contenente dati utente `cloud-init` nel formato `cloud-config`.

`guestinfo.vendordata` (facoltativo)

YAMLcontenente dati del `cloud-init` fornitore

Le proprietà di codifica corrispondenti (`guestinfo.metadata.encoding`, `guestinfo.userdata.encoding` e `guestinfo.vendordata.encoding`) possono contenere:

`base64`

Il contenuto della proprietà è codificato con `base64`.

`gzip+base64`

Il contenuto della proprietà è compresso con `gzip` dopo la codifica con `base64`.

> **Note**
>
> Il `seed.iso` metodo supporta un file di `network-config` configurazione separato (opzionale). VMware`guestinfo`differisce nel modo in cui viene fornita la configurazione di rete. Ulteriori informazioni sono fornite nella sezione seguente.

Se desideri una configurazione di rete esplicita, devi incorporarla in `metadata` sotto forma di due proprietà YAML o JSON:

`network`

Contiene la configurazione di rete codificata in formato JSON o YAML.

`network.encoding`

Contiene la codifica dei suddetti dati di configurazione di rete. Le codifiche supportate da `cloud-init` sono le stesse dei dati `guestinfo`: `base64` e `gzip+base64`.

Example Utilizzo dello strumento VMware vSphere **`govc`** CLI per passare la configurazione con **`guestinfo`**

1. Preparare `meta-data` i `user-data` file di `network-config` configurazione e quelli opzionali come descritto in. [NoCloud (`seed.iso`) `cloud-init` configurazione per Amazon Linux 2023 su KVM e VMware]
2. Convertire i file di configurazione in formati utilizzabili da VMware`guestinfo`.

```
# 'meta-data', `user-data` and `network-config` are the configuration
# files in the same format that would be used by a NoCloud (seed.iso)
# data source, read-them and convert them to VMware guestinfo
#
# The VM_NAME variable is assumed to be set to the name of the VM
# It is assumed that the necessary govc environment (credentials etc...) are
 already set

metadata=$(cat "meta-data")
userdata=$(cat "user-data")
if [ -e "network-config" ] ; then
    # We need to embed the network config inside the meta-data
    netconf=$(base64 -w0 "network-config")
```

```
    metadata=$(printf "%s\nnetwork: %s\nnetwork.encoding: base64" "$metadata"
 "$netconf")
fi
metadata=$(base64 -w0 <<< "$metadata")
govc vm.change -vm "$VM_NAME" \
    -e guestinfo.metadata="$metadata" \
    -e guestinfo.metadata.encoding="base64"
userdata=$(base64 -w0 <<< "$userdata")
govc vm.change -vm "$VM_NAME" \
    -e guestinfo.userdata="$userdata" \
    -e guestinfo.userdata.encoding="base64"
```

Confronto dei pacchetti installati sull'AMI standard di Amazon Linux 2023 con l'immagine KVM AL2023

Un confronto tra gli RPM presenti sull'AMI standard AL2023 rispetto agli RPM presenti sull'immagine KVM AL2023.

Pacchetto	AMI	KVM
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023,420240319
amazon-linux-repo-s3	2023,420240319	
amazon-linux-sb-keys	2023,1	2023,1
amazon-onprem-network		1.2

Pacchetto	AMI	KVM
amazon-rpm-config	228	228
amazon-ssm-agent	3,2,2303,0	3,2233,0
at	3,1,23	3,1,23
attr	2.5.1	2.5.1
audit	30,6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2.0	
awscli-2	2.14.5	2.14.5
basesystem	11	11
bash	5,2,15	5,2,15
bash-completion	2.11	2.11
bc	1,07,1	1,07,1
bind-libs	9,16,48	9,16,48
bind-license	9,16,48	9,16,48
bind-utils	9,16,48	9,16,48
binutils	2,39	2,39
boost-filesystem	1,75,0	1,75,0
boost-system	1,75,0	1,75,0
boost-thread	1,75,0	1,75,0
bzip2	1.0.8	1.0.8

Pacchetto	AMI	KVM
bzip2-libs	1.0.8	1.0.8
c-ares	1.19.0	
ca-certificates	2023,2,64	2023,2,64
checkpolicy	3.4	3.4
chkconfig	1.15	1.15
chrony	4.3	4.3
cloud-init	222,2	222,2
cloud-init-cfg-ec2	222,2	
cloud-init-cfg-onprem		222,2
cloud-utils-growpart	0,31	0,31
coreutils	8,32	8,32
coreutils-common	8,32	8,32
cpio	2,13	2,13
cracklib	2,9,6	29.6
cracklib-dicts	29.6	29.6
crontabs	1.11	1.11
crypto-policies	20220428	20220428
crypto-policies-scripts	20220428	20220428
cryptsetup	2.6.1	2.6.1
cryptsetup-libs	2.6.1	2.6.1

Pacchetto	AMI	KVM
curl-minimal	8,5,0	8,5,0
cyrus-sasl-lib	2,1,27	2,1,27
cyrus-sasl-plain	2,1,27	2,1,27
dbus	1,12,28	1,12,28
dbus-broker	32	32
dbus-common	1,12,28	1,12,28
dbus-libs	1,12,28	1,12,28
device-mapper	1,02,185	1,02,185
device-mapper-libs	1,02,185	1,02,185
diffutils	3.8	3.8
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugin-support-info	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2
dracut	055	055
dracut-config-ec2	3.0	
dracut-config-generic	055	055

Pacchetto	AMI	KVM
dwz	0,14	0,14
dyninst	102,1	10.2.1
e2fsprogs	1,446,5	1,46,5
e2fsprogs-libs	1,46,5	1,46,5
ec2-hibinit-agent	1.0.8	
ec2-instance-connect	1.1	
ec 2- instance-connect-selinux	1.1	
ec2-utils	2.2.0	
ed	1.14.2	1.14.2
efi-filesystem	5	5
efi-srpm-macros	5	5
efivar	38	38
efivar-libs	38	38
elfutils-debuginfod-client	0.188	0.188
elfutils-default-yama-scope	0.188	0.188
elfutils-libelf	0.188	0.188
elfutils-libs	0.188	0.188
ethtool	5,15	5,15
expat	2.5.0	2.5.0
file	5,39	5,39

Pacchetto	AMI	KVM
file-libs	5,39	5,39
filesystem	3,14	3,14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5
fstrm	0.6.1	0.6.1
fuse-libs	2,9,9	29.9
gawk	5.1.0	5.1.0
gdbm-libs	1,19	1,19
gdisk	1.0.8	1.0.8
gettext	0,21	0,21
gettext-libs	0,21	0,21
ghc-srpm-macros	1.5.0	1.5.0
glib2	2,74,7	2,74,7
glibc	2,34	2,34
glibc-all-langpacks	2,34	2,34
glibc-common	2,34	2,34
glibc-gconv-extra	2,34	2,34
glibc-locale-source	2,34	2,34
gmp	62,1	6.2.1
gnupg2-minimal	2.3.7	2.3.7

Pacchetto	AMI	KVM
gnutls	3.8.0	3.8.0
go-srpm-macros	3.2.0	3.2.0
gpgme	1.15.1	1.15.1
gpm-libs	1,20.7	1,20.7
grep	3.8	3.8
groff-base	1,22,4	1,22,4
grub2-common	2,06	2,06
grub2-efi-aa64-ec2	2,06 (aarch64)	2.06 (aarch64)
grub2-efi-x64-ec2	2,06 (x86_64)	2,06 (x86_64)
grub2-pc		2,06 (x86_64)
grub2-pc-modules	2,06	2.06 (nomarzo)
grub2-tools	2.06	2,06
grub2-tools-minimal	2,06	2,06
grubby	8,40	8,40
gssproxy	0.8.4	0.8.4
gzip	1.12	1.12
hostname	3,23	3,23
hunspell	1.7.0	1.7.0
hunspell-en	0,20140811,1	0,20140811,1
hunspell-en-GB	0,20140811,1	0,20140811,1

Pacchetto	AMI	KVM
hunspell-en-US	0,20140811,1	0,20140811,1
hunspell-filesystem	1.7.0	1.7.0
hwdata	0,3353	0,3353
Info	6.7	6.7
inih	49	49
initscripts	10,09	10,09
iproute	5.10.0	5.10.0
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0
jansson	2.14	2.14
jitterentropy	3.4.1	3.4.1
jq	1.7.1	
json-c	0,14	0,14
kbd	2.4.0	2.4.0
kbd-misc	2.4.0	2.4.0
kernel	61,79	6,1,79
kernel-livepatch-repo-cdn		2023,420240319
kernel-livepatch-repo-s3	2023,420240319	
kernel-modules-extra		6,1,79
kernel-modules-extra-common		6,1,79

Pacchetto	AMI	KVM
kernel-srpm-macros	1.0	1
kernel-tools	6,1,79	6,1,79
keyutils	1.6.3	1.6.3
keyutils-libs	1.6.3	1.6.3
kmod	29	29
kmod-libs	29	29
kpatch-runtime	0,9,7	0,9,7
krb5-libs	1,21	1,21
less	608	608
libacl	2.3.1	2.3.1
libaio	0,3111	0,3111
libarchive	3,5,3	3,5,3
libargon2	20171227	20171227
libassuan	2,5,5	2,5,5
libattr	2.5.1	2.5.1
libbasicobjects	0,11	01.1
libblkid	2,37,4	2,37,4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0

Pacchetto	AMI	KVM
libcollection	0.7.0	0.7.0
libcom_err	1,446,5	1,46,5
libcomps	01,20	01,20
libconfig	17.2	1.7.2
libcurl-minimal	8,5,0	8,5,0
libdb	5,3,28	5,3,28
libdhash	0,50	
libdnf	0,69,0	0,69,0
libeconf	0,40	0,40
libedit	3.1	3.1
libev	4,33	4,33
libevent	2,1,12	2,1,12
libfdisk	2,37,4	2,37,4
libffi	34.4	34.4
libfido2	1.10.0	1.10.0
libgcc	114,1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1,42	1,42
libibverbs	48,0	48,0

Pacchetto	AMI	KVM
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmaccalc	1.4.0	1.4.0
libldb	26.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0,13	0,13
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2,37,4	2,37,4
libnfsidmap	2,5,4	2.5.4
libnghttp2	1,57,0	1,57,0
libnl3	3.5.0	3.5.0
libpath_utils	0,2,1	0,2,1
libpcap	1.10.1	1.10.1
libpipeline	1.5.3	1.5.3
libpkgconf	1.8.0	1.8.0
libpsl	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4
libref_array	0,1,5	0,1,5

Pacchetto	AMI	KVM
librepo	1,14,5	1,14,5
libreport-filesystem	2,15,2	2,15,2
libseccomp	2.5.3	2.5.3
libselinux	3.4	3.4
libselinux-utils	3.4	3.4
libsemanage	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2,13	2,13
libsmartcols	2,37,4	2,37,4
libsolv	0,7,22	0,7,22
libss	1,446,5	1,46,5
libsss_certmap	2,9,4	
libsss_idmap	2,9,4	2,9,4
libsss_nss_idmap	2,9,4	2,9,4
libsss_sudo	2.9.4	
libstdc++	11.4.1	11.4.1
libstoragemgmt	1.9.4	1.9.4
libtalloc	2.3.4	
libtasn1	4,19,0	4,19,0
libtdb	1.4.7	

Pacchetto	AMI	KVM
libtevent	0.13.0	
libtextstyle	0,21	0,21
libtirpc	1.3.3	1.3.3
libunistring	0,9,10	0,9,10
libuser	0,63	0,63
libutempter	1.2.1	1.2.1
libuuid	2,37,4	2,37,4
libuv	1.47.0	1.47.0
libverto	0,32	0,32
libverto-libev	0,32	0,32
libxcrypt	4,4,33	4,4,33
libxml2	2,10,4	210.4
libyaml	02,5	02,5
libzstd	1,5,5	1,5,5
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0,9,29	0,9,29
logrotate	3,20,1	3,20,1
lsof	4,94,0	4,94,0
lua-libs	5.4.4	5.4.4
lua-srpm-macros	1	1

Pacchetto	AMI	KVM
lz4-libs	1.9.4	1.9.4
man-db	2,9,3	29.3
man-pages	5,10	5,10
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)
mpfr	4.1.0	4.1.0
nano	5.8	5.8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
net-tools	2.0	2.0
nettle	3.8	3.8
newt	0,52,21	0,52,21
nfs-utils	2,5,4	2.5.4
npth	1.6	1.6
nspr	4,35,0	4,35,0
nss	3,90,0	3,90,0
nss-softokn	3,90,0	3,90,0
nss-softokn-freebl	3,90,0	3,90,0
nss-sysinit	3,90,0	3,90,0
nss-util	3,90,0	3,90,0

Pacchetto	AMI	KVM
ntsysv	1.15	1.15
numactl-libs	2.0,14	2.0,14
ocaml-srpm-macros	6	6
oniguruma	6,9,7,1	
openblas-srpm-macros	2	2
openldap	2,4,57	2,4,57
openssh	8.7p1	8,7p1
openssh-clients	8,7p1	8,7p1
openssh-server	8,7p1	8,7p1
openssl	3,0,8	30,8
openssl-libs	30,8	30,8
openssl-pkcs11	0,4,12	0,4,12
os-prober	1,77	1,77
p11-kit	0,24,1	0,24,1
p11-kit-trust	0,24,1	0,24,1
package-notes-srpm-macros	0.4	0.4
pam	1.5.1	1.5.1
parted	3.4	3.4
passwd	0,80	0,80
pciutils	3.7.0	3.7.0

Pacchetto	AMI	KVM
pciutils-libs	3.7.0	3.7.0
pcre2	10,40	10,40
pcre2-syntax	10,40	10,40
perl-Carp	1,50	1,50
perl-Class-Struct	0,66	0,66
perl- DynaLoader	1,47	1,47
perl-Encode	3,15	3,15
perl-Errno	1,30	1,30
perl-Exporter	5,74	5,74
perl-Fcntl	1.13	1.13
perl-File-Basename	2,85	2,85
perl-File-Path	2,18	2,18
perl-File-Temp	0,231,100	0,231,100
perl-File-stat	1,09	1,09
perl-Getopt-Long	2,52	2,52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-IO	1,43	1,43
perl-IPC-Open3	1,21	1,21
perl-MIME-Base64	3,16	3,16

Pacchetto	AMI	KVM
perl-POSIX	1,94	1,94
perl- PathTools	3,78	3,78
perl-Pod-Escapes	1,07	1,07
perl-Pod-Perldoc	3,28,01	3,28,01
perl-Pod-Simple	3,42	3,42
perl-Pod-Usage	2,01	2,01
perl-Scalar-List-Utils	1,56	1,56
perl- SelectSaver	1.02	1.02
perl-Socket	2.032	2,032
perl-Storable	3,21	3,21
perl-Symbol	1,08	1,08
perl-Term-ANSIColor	5,01	5,01
perl-Term-Cap	1,17	1,17
Testo in Perl- ParseWords	3.30	3,30
perl-Text-Tabs+Wrap	2021,0726	2021,0726
perl-Time-Local	1,300	1.300
perl-constant	1,33	1,33
perl-if	0,60,800	0,60,800
perl-interpreter	5,32,1	5,32,1
perl-libs	5,32,1	5,32,1

Pacchetto	AMI	KVM
perl-mro	1,23	1,23
perl-overload	1,31	1,31
perl-overloading	0,02	0,02
perl-parent	0,238	0,238
perl-podlators	4,14	4,14
perl-srpm-macros	1	1
perl-subs	1,03	1,03
perl-vars	1,05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4
policycoreutils-python-utils	3.4	
popt	1,18	1,18
procps-ng	3,3,17	3,3,17
protobuf-c	1.4.1	1.4.1
psacct	6,6,4	6.6.4
psmisc	23,4	23,4
publicsuffix-list-dafsa	20240212	20240212
python-chevron	0.13.1	

Pacchetto	AMI	KVM
python-srpm-macros	3.9	3.9
python3	3,9,16	3,9,16
python3-attrs	20,3,0	20,3,0
python3-audit	30.6	3.0.6
python3-awscrt	0,19,19	0,19,19
python3-babel	2,9,1	29.1
python3-cffi	1,14,5	1,14,5
python3-chardet	4.0.0	4.0.0
python3-colorama	04.4	04.4
python3-configobj	50.6	5.0.6
python3-cryptography	36,0	36,0
python3-daemon	2.3.0	
python3-dateutil	28.1	28.1
python3-dbus	1,2,18	1,2,18
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python 3- dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1
python3-hawkey	0,69,0	0,69,0

Pacchetto	AMI	KVM
python3-idna	(2.10)	(2.10)
python3-jinja2	211,3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1,21	1,21
python3-jsonpointer	2.0	2.0
python3-jsonschema	3.2.0	3.2.0
python3-libcomps	01,20	01,20
python3-libdnf	0,69,0	0,69,0
python3-libs	3,9,16	3,9,16
python3-libselinux	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstoragemgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0,10,6	0,10,6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21,31	21,31
python3-ply	3,11	3,11
python3-policycoreutils	3.4	3.4
python3-prettytable	0.7.2	0.7.2

Pacchetto	AMI	KVM
python3-prompt-toolkit	3,0,24	3,0,24
python3-pycparser	2,20	2,20
python3-pyrsistent	0,17,3	0,17,3
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022,7,1	2022,7,1
python3-pyyaml	5.4.1	5.4.1
python3-requests	2,25,1	2,25,1
python3-rpm	4,161,3	4,161,3
python3-ruamel-yaml	0,16,6	0,16,6
pitone 3- ruamel-yaml-clib	0.1.2	0,1,2
python3-setools	4.4.1	4.4.1
python3-setuptools	59,60	59,6,0
python3-setuptools-wheel	59,6,0	59,6,0
python3-six	1.15.0	1.15.0
sistema python3	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0,2,5	02,5
quota	4,06	4,06
quota-nls	4,06	4,06

Pacchetto	AMI	KVM
readline	8.1	8.1
rng-tools	6,14	6,14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4,161,3	4,161,3
rpm-build-libs	4,161,3	4,161,3
rpm-libs	4,161,3	4,161,3
rpm-plugin-selinux	4,161,3	4,161,3
rpm-plugin-systemd-inhibit	4,161,3	4,161,3
rpm-sign-libs	4,161,3	4,161,3
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	37,22	37,22
selinux-policy-targeted	37,22	37,22
setup	2,13,7	2,13,7
shadow-utils	4.9	4.9
slang	2.3.2	2.3.2

Pacchetto	AMI	KVM
sqlite-libs	3,4,0	3,4,0
sssd-client	2,9,4	2,9,4
sssd-common	2,9,4	
sssd-kcm	2,9,4	
sssd-nfs-idmap	2,9,4	
strace	5,16	5,16
sudo	1,9,14	1,9,14
sysctl-defaults	1.0	1
sysstat	12,5,6	12,5,6
system-release	2023,420240319	2023,420240319
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
systemtap-runtime	4,8	4.8
tar	1,34	1,34
tbb	2020,3	2020,3
tcpdump	4,99,1	4,99,1

Pacchetto	AMI	KVM
tcsh	6,24,07	6,24,07
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2
userspace-rcu	0.12.1	0.12.1
util-linux	2,37,4	2,37,4
util-linux-core	2,37,4	2,37,4
vim-common	9,0,2153	9,0,2153
vim-data	9,0,2153	9,0,2153
vim-enhanced	9,0,2153	9,0,2153
vim-filesystem	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153
wget	1,21,3	1,21,3
which	2,21	2,21
words	3.0	3.0
xfsdump	3,1,11	3,1,11
xfsprogs	5,18,0	5,18,0
xxd	9,0,2153	9,0,2153

Pacchetto	AMI	KVM
xxhash-libs	0.8.0	0.8.0
xz	52,5	5.2.5
xz-libs	5.2.5	5.2.5
yum	4.14.0	4.14.0
zip	3.0	3.0
zlib	1,2,11	1,2,11
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	
zstd	1,5,5	1,5,5

Confronto dei pacchetti installati sull'AMI standard di Amazon Linux 2023 con l'immagine OVA VMware AL2023

Un confronto tra gli RPM presenti sull'AMI standard AL2023 rispetto agli RPM presenti sull'immagine AL2023 VMware OVA.

Pacchetto	AMI	VMware OVA
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2

Pacchetto	AMI	VMware OVA
amazon-linux-repo-cdn		2023,420240319
amazon-linux-repo-s3	2023,420240319	
amazon-linux-sb-keys	2023,1	2023,1
amazon-onprem-network		1.2
amazon-rpm-config	228	228
amazon-ssm-agent	3,2,2303,0	3,2233,0
at	3,1,23	3,1,23
attr	2.5.1	2.5.1
audit	30,6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2.0	
awscli-2	2.14.5	2.14.5
basesystem	11	11
bash	5,2,15	5,2,15
bash-completion	2.11	2.11
bc	1,07,1	1,07,1
bind-libs	9,16,48	9,16,48
bind-license	9,16,48	9,16,48
bind-utils	9,16,48	9,16,48
binutils	2,39	2,39

Pacchetto	AMI	VMware OVA
boost-filesystem	1,75,0	1,75,0
boost-system	1,75,0	1,75,0
boost-thread	1,75,0	1,75,0
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
c-ares	1.19.0	
ca-certificates	2023,2,64	2023,2,64
checkpolicy	3.4	3.4
chkconfig	1.15	1.15
chrony	4.3	4.3
cloud-init	222,2	222,2
cloud-init-cfg-ec2	222,2	
cloud-init-cfg-onprem		222,2
cloud-utils-growpart	0,31	0,31
coreutils	8,32	8,32
coreutils-common	8,32	8,32
cpio	2,13	2,13
cracklib	2,9,6	29.6
cracklib-dicts	29.6	29.6
crontabs	1.11	1.11

Pacchetto	AMI	VMware OVA
crypto-policies	20220428	20220428
crypto-policies-scripts	20220428	20220428
cryptsetup	2.6.1	2.6.1
cryptsetup-libs	2.6.1	2.6.1
curl-minimal	8,5,0	8,5,0
cyrus-sasl-lib	2,1,27	2,1,27
cyrus-sasl-plain	2,1,27	2,1,27
dbus	1,12,28	1,12,28
dbus-broker	32	32
dbus-common	1,12,28	1,12,28
dbus-libs	1,12,28	1,12,28
device-mapper	1,02,185	1,02,185
device-mapper-libs	1,02,185	1,02,185
diffutils	3.8	3.8
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugin-support-info	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-utils	4.3.0	4.3.0

Pacchetto	AMI	VMware OVA
dosfstools	4.2	4.2
dracut	055	055
dracut-config-ec2	3.0	
dracut-config-generic	055	055
dwz	0,14	0,14
dyninst	102,1	10.2.1
e2fsprogs	1,446,5	1,46,5
e2fsprogs-libs	1,46,5	1,46,5
ec2-hibinit-agent	1.0.8	
ec2-instance-connect	1.1	
ec 2- instance-connect-selinux	1.1	
ec2-utils	2.2.0	
ed	1.14.2	1.14.2
efi-filesystem	5	5
efi-srpm-macros	5	5
efivar	38	38
efivar-libs	38	38
elfutils-debuginfod-client	0.188	0.188
elfutils-default-yama-scope	0.188	0.188
elfutils-libelf	0.188	0.188

Pacchetto	AMI	VMware OVA
elfutils-libs	0.188	0.188
ethtool	5,15	5,15
expat	2.5.0	2.5.0
file	5,39	5,39
file-libs	5,39	5,39
filesystem	3,14	3,14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5
fstrm	0.6.1	0.6.1
fusibile comune		3.10.4
fuse-libs	2,9,9	29.9
fuse3		3.10.4
fuse3-libs		3.10.4
gawk	5.1.0	5.1.0
gdbm-libs	1,19	1,19
gdisk	1.0.8	1.0.8
gettext	0,21	0,21
gettext-libs	0,21	0,21
ghc-srpm-macros	1.5.0	1.5.0
glib2	2,74,7	2,74,7

Pacchetto	AMI	VMware OVA
glibc	2,34	2,34
glibc-all-langpacks	2,34	2,34
glibc-common	2,34	2,34
glibc-gconv-extra	2,34	2,34
glibc-locale-source	2,34	2,34
gmp	62,1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gnutls	3.8.0	3.8.0
go-srpm-macros	3.2.0	3.2.0
gpgme	1.15.1	1.15.1
gpm-libs	1,20.7	1,20.7
grep	3.8	3.8
groff-base	1,22,4	1,22,4
grub2-common	2,06	2,06
grub2-efi-x64-ec2	2,06	2,06
grub2-pc		2,06
grub2-pc-modules	2,06	2,06
grub2-tools	2,06	2,06
grub2-tools-minimal	2,06	2,06
grubby	8,40	8,40

Pacchetto	AMI	VMware OVA
gssproxy	0.8.4	0.8.4
gzip	1.12	1.12
hostname	3,23	3,23
hunspell	1.7.0	1.7.0
hunspell-en	0,20140811,1	0,20140811,1
hunspell-en-GB	0,20140811,1	0,20140811,1
hunspell-en-US	0,20140811,1	0,20140811,1
hunspell-filesystem	1.7.0	1.7.0
hwdata	0,3353	0,353
Info	6.7	6.7
inih	49	49
initscripts	10,09	10,09
iproute	5.10.0	5.10.0
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0
jansson	2.14	2.14
jitterentropy	3.4.1	3.4.1
jq	1.7.1	
json-c	0,14	0,14
kbd	2.4.0	2.4.0

Pacchetto	AMI	VMware OVA
kbd-misc	2.4.0	2.4.0
kernel	61,79	6,1,79
kernel-livepatch-repo-cdn		2023,420240319
kernel-livepatch-repo-s3	2023,420240319	
kernel-modules-extra		6,1,79
kernel-modules-extra-common		6,1,79
kernel-srpm-macros	1.0	1
kernel-tools	6,1,79	6,1,79
keyutils	1.6.3	1.6.3
keyutils-libs	1.6.3	1.6.3
kmod	29	29
kmod-libs	29	29
kpatch-runtime	0,9,7	0,9,7
krb5-libs	1,21	1,21
less	608	608
libacl	2.3.1	2.3.1
libaio	0,3111	0,3111
libarchive	3,5,3	3,5,3
libargon2	20171227	20171227
libassuan	2,5,5	2,5,5

Pacchetto	AMI	VMware OVA
libattr	2.5.1	2.5.1
libbasicobjects	0,11	01.1
libblkid	2,37,4	2,37,4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1,446,5	1,46,5
libcomps	01,20	01,20
libconfig	17.2	1.7.2
libcurl-minimal	8,5,0	8,5,0
libdb	5,3,28	5,3,28
libdhash	0,50	
libdnf	0,69,0	0,69,0
libeconf	0,40	0,40
libedit	3.1	3.1
libev	4,33	4,33
libevent	2,1,12	2,1,12
libfdisk	2,37,4	2,37,4
libffi	34.4	34.4

Pacchetto	AMI	VMware OVA
libfido2	1.10.0	1.10.0
libgcc	114,1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1,42	1,42
libibverbs	48,0	48,0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmaccalc	1.4.0	1.4.0
libldb	26.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0,13	0,13
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2,37,4	2,37,4
pacchetto libm		0.10.1
libnfsidmap	2,5,4	2.5.4
libnghttp2	1,57,0	1,57,0
libnl3	3.5.0	3.5.0

Pacchetto	AMI	VMware OVA
libpath_utils	0,2,1	0,2,1
libpcap	1.10.1	1.10.1
libpipeline	1.5.3	1.5.3
libpkgconf	1.8.0	1.8.0
libpsl	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4
libref_array	0,1,5	0,1,5
librepo	1,14,5	1,14,5
libreport-filesystem	2,15,2	2,15,2
libseccomp	2.5.3	2.5.3
libselinux	3.4	3.4
libselinux-utils	3.4	3.4
libsemanage	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2,13	2,13
libsmartcols	2,37,4	2,37,4
libsolv	0,7,22	0,7,22
libss	1,446,5	1,46,5
libsss_certmap	2,9,4	
libsss_idmap	2,9,4	2,9,4

Pacchetto	AMI	VMware OVA
libsss_nss_idmap	2,9,4	2,9,4
libsss_sudo	2.9.4	
libstdc++	11.4.1	11.4.1
libstoragemgmt	1.9.4	1.9.4
libtalloc	2.3.4	
libtasn1	4,19,0	4,19,0
libtdb	1.4.7	
libtevent	0.13.0	
libtextstyle	0,21	0,21
libtirpc	1.3.3	1.3.3
libtool-ltdl		2.4.7
libunistring	0.9.10	0,9,10
libuser	0,63	0,63
libutempter	1.2.1	1.2.1
libuuid	2,37,4	2,37,4
libuv	1.47.0	1.47.0
libverto	0,32	0,32
libverto-libev	0,32	0,32
libxcrypt	4,4,33	4,4,33
libxml2	2,10,4	210.4

Pacchetto	AMI	VMware OVA
libxslt		1,1,34
libyaml	0,2,5	02,5
libzstd	1,5,5	1,5,5
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0,9,29	0,9,29
logrotate	3,20,1	3,20,1
lsof	4,94,0	4,94,0
lua-libs	5.4.4	5.4.4
lua-srpm-macros	1	1
lz4-libs	1.9.4	1.9.4
man-db	2,9,3	29.3
man-pages	5,10	5,10
microcode_ctl	2.1	2.1
mpfr	4.1.0	4.1.0
nano	5.8	5.8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
net-tools	2.0	2.0
nettle	3.8	3.8

Pacchetto	AMI	VMware OVA
newt	0,52,21	0,52,21
nfs-utils	2,5,4	2.5.4
npth	1.6	1.6
nspr	4,35,0	4,35,0
nss	3,90,0	3,90,0
nss-softokn	3,90,0	3,90,0
nss-softokn-freebl	3,90,0	3,90,0
nss-sysinit	3,90,0	3,90,0
nss-util	3,90,0	3,90,0
ntsysv	1.15	1.15
numactl-libs	2.0,14	2.0,14
ocaml-srpm-macros	6	6
oniguruma	6,9,7,1	
open-vm-tools		12,3,0
openblas-srpm-macros	2	2
openldap	2,4,57	2,4,57
openssh	8.7p1	8,7p1
openssh-clients	8,7p1	8,7p1
openssh-server	8,7p1	8,7p1
openssl	3,0,8	30,8

Pacchetto	AMI	VMware OVA
openssl-libs	30,8	30,8
openssl-pkcs11	0,4,12	0,4,12
os-prober	1,77	1,77
p11-kit	0,24,1	0,24,1
p11-kit-trust	0,24,1	0,24,1
package-notes-srpm-macros	0.4	0.4
pam	1.5.1	1.5.1
parted	3.4	3.4
passwd	0,80	0,80
pciutils	3.7.0	3.7.0
pciutils-libs	3.7.0	3.7.0
pcre2	10,40	10,40
pcre2-syntax	10,40	10,40
perl-Carp	1,50	1,50
perl-Class-Struct	0,66	0,66
perl- DynaLoader	1,47	1,47
perl-Encode	3,15	3,15
perl-Errno	1,30	1,30
perl-Exporter	5,74	5,74
perl-Fcntl	1.13	1.13

Pacchetto	AMI	VMware OVA
perl-File-Basename	2,85	2,85
perl-File-Path	2,18	2,18
perl-File-Temp	0,231,100	0,231,100
perl-File-stat	1,09	1,09
perl-Getopt-Long	2,52	2,52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-IO	1,43	1,43
perl-IPC-Open3	1,21	1,21
perl-MIME-Base64	3,16	3,16
perl-POSIX	1,94	1,94
perl- PathTools	3,78	3,78
perl-Pod-Escapes	1,07	1,07
perl-Pod-Perldoc	3,28,01	3,28,01
perl-Pod-Simple	3,42	3,42
perl-Pod-Usage	2,01	2,01
perl-Scalar-List-Utils	1,56	1,56
perl- SelectSaver	1.02	1.02
perl-Socket	2.032	2,032
perl-Storable	3,21	3,21

Pacchetto	AMI	VMware OVA
perl-Symbol	1,08	1,08
perl-Term-ANSIColor	5,01	5,01
perl-Term-Cap	1,17	1,17
Testo in Perl- ParseWords	3.30	3,30
perl-Text-Tabs+Wrap	2021,0726	2021,0726
perl-Time-Local	1,300	1.300
perl-constant	1,33	1,33
perl-if	0,60,800	0,60,800
perl-interpreter	5,32,1	5,32,1
perl-libs	5,32,1	5,32,1
perl-mro	1,23	1,23
perl-overload	1,31	1,31
perl-overloading	0,02	0,02
perl-parent	0,238	0,238
perl-podlators	4,14	4,14
perl-srpm-macros	1	1
perl-subs	1,03	1,03
perl-vars	1,05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0

Pacchetto	AMI	VMware OVA
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4
policycoreutils-python-utils	3.4	
popt	1,18	1,18
procps-ng	3,3,17	3,3,17
protobuf-c	1.4.1	1.4.1
psacct	6,6,4	6.6.4
psmisc	23,4	23,4
publicsuffix-list-dafsa	20240212	20240212
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
python3	3,9,16	3,9,16
python3-attrs	20,3,0	20,3,0
python3-audit	30.6	3.0.6
python3-awscrt	0,19,19	0,19,19
python3-babel	2,9,1	29.1
python3-cffi	1,14,5	1,14,5
python3-chardet	4.0.0	4.0.0
python3-colorama	04.4	04.4
python3-configobj	50.6	5.0.6

Pacchetto	AMI	VMware OVA
python3-cryptography	36,0	36,0
python3-daemon	2.3.0	
python3-dateutil	28.1	28.1
python3-dbus	1,2,18	1,2,18
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python 3- dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1
python3-hawkey	0,69,0	0,69,0
python3-idna	(2.10)	(2.10)
python3-jinja2	211,3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1,21	1,21
python3-jsonpointer	2.0	2.0
python3-jsonschema	3.2.0	3.2.0
python3-libcomps	01,20	01,20
python3-libdnf	0,69,0	0,69,0
python3-libs	3,9,16	3,9,16
python3-libselinux	3.4	3.4

Pacchetto	AMI	VMware OVA
python3-libsemanage	3.4	3.4
python3-libstoragemgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0,10,6	0,10,6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21,31	21,31
python3-ply	3,11	3,11
python3-policycoreutils	3.4	3.4
python3-prettytable	0.7.2	0.7.2
python3-prompt-toolkit	3,0,24	3,0,24
python3-pycparser	2,20	2,20
python3-pyrsistent	0,17,3	0,17,3
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022,7,1	2022,7,1
python3-pyyaml	5.4.1	5.4.1
python3-requests	2,25,1	2,25,1
python3-rpm	4,161,3	4,161,3
python3-ruamel-yaml	0,16,6	0,16,6

Pacchetto	AMI	VMware OVA
pitone 3- ruamel-yaml-clib	0.1.2	0,1,2
python3-setools	4.4.1	4.4.1
python3-setuptools	59,60	59,6,0
python3-setuptools-wheel	59,6,0	59,6,0
python3-six	1.15.0	1.15.0
sistema python3	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0,2,5	02,5
quota	4,06	4,06
quota-nls	4,06	4,06
readline	8.1	8.1
rng-tools	6,14	6,14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4,161,3	4,161,3
rpm-build-libs	4,161,3	4,161,3
rpm-libs	4,161,3	4,161,3
rpm-plugin-selinux	4,161,3	4,161,3
rpm-plugin-systemd-inhibit	4,161,3	4,161,3
rpm-sign-libs	4,161,3	4,161,3

Pacchetto	AMI	VMware OVA
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	37,22	37,22
selinux-policy-targeted	37,22	37,22
setup	2,13,7	2,13,7
shadow-utils	4.9	4.9
slang	2.3.2	2.3.2
sqlite-libs	3,4,0	3,4,0
sssd-client	2,9,4	2,9,4
sssd-common	2,9,4	
sssd-kcm	2,9,4	
sssd-nfs-idmap	2,9,4	
strace	5,16	5,16
sudo	1,9,14	1,9,14
sysctl-defaults	1.0	1
sysstat	12,5,6	12,5,6
system-release	2023,420240319	2023,420240319

Pacchetto	AMI	VMware OVA
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
systemtap-runtime	4,8	4.8
tar	1,34	1,34
tbb	2020,3	2020,3
tcpdump	4,99,1	4,99,1
tcsh	6,24,07	6,24,07
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2
userspace-rcu	0.12.1	0.12.1
util-linux	2,37,4	2,37,4
util-linux-core	2,37,4	2,37,4
vim-common	9,0,2153	9,0,2153

Pacchetto	AMI	VMware OVA
vim-data	9,0,2153	9,0,2153
vim-enhanced	9,0,2153	9,0,2153
vim-filesystem	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153
wget	1,21,3	1,21,3
which	2,21	2,21
words	3.0	3.0
xfsdump	3,1,11	3,1,11
xfsprogs	5,18,0	5,18,0
xml sec1		1.2.33
xmlsec1-openssl		1.2.33
xxd	9,0,2153	9,0,2153
xxhash-libs	0.8.0	0.8.0
xz	52,5	5.2.5
xz-libs	5.2.5	5.2.5
yum	4.14.0	4.14.0
zip	3.0	3.0
zlib	1,2,11	1,2,11
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	

Pacchetto	AMI	VMware OVA
zstd	1,5,5	1,5,5

Confronto dei pacchetti installati sull'AMI standard di Amazon Linux 2023 con l'immagine Hyper-V AL2023

Un confronto tra gli RPM presenti sull'AMI standard AL2023 rispetto agli RPM presenti sull'immagine AL2023 Hyper-V.

Pacchetto	AMI	VHDX Hyper-V
acl	2.3.1	2.3.1
acpid	2,0,32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023,420240319
amazon-linux-repo-s3	2023,420240319	
amazon-linux-sb-keys	2023,1	2023,1
amazon-onprem-network		1.2
amazon-rpm-config	228	228
amazon-ssm-agent	3,2,2303,0	3,2233,0
at	3,1,23	3,1,23
attr	2.5.1	2.5.1

Pacchetto	AMI	VHDX Hyper-V
audit	30,6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2.0	
awscli-2	2.14.5	2.14.5
basesystem	11	11
bash	5,2,15	5,2,15
bash-completion	2.11	2.11
bc	1,07,1	1,07,1
bind-libs	9,16,48	9,16,48
bind-license	9,16,48	9,16,48
bind-utils	9,16,48	9,16,48
binutils	2,39	2,39
boost-filesystem	1,75,0	1,75,0
boost-system	1,75,0	1,75,0
boost-thread	1,75,0	1,75,0
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
c-ares	1.19.0	
ca-certificates	2023,2,64	2023,2,64
checkpolicy	3.4	3.4

Pacchetto	AMI	VHDX Hyper-V
chkconfig	1.15	1.15
chrony	4.3	4.3
cloud-init	222,2	222,2
cloud-init-cfg-ec2	222,2	
cloud-init-cfg-onprem		222,2
cloud-utils-growpart	0,31	0,31
coreutils	8,32	8,32
coreutils-common	8,32	8,32
cpio	2,13	2,13
cracklib	2,9,6	29.6
cracklib-dicts	29.6	29.6
crontabs	1.11	1.11
crypto-policies	20220428	20220428
crypto-policies-scripts	20220428	20220428
cryptsetup	2.6.1	2.6.1
cryptsetup-libs	2.6.1	2.6.1
curl-minimal	8,5,0	8,5,0
cyrus-sasl-lib	2,1,27	2,1,27
cyrus-sasl-plain	2,1,27	2,1,27
dbus	1,12,28	1,12,28

Pacchetto	AMI	VHDX Hyper-V
dbus-broker	32	32
dbus-common	1,12,28	1,12,28
dbus-libs	1,12,28	1,12,28
device-mapper	1,02,185	1,02,185
device-mapper-libs	1,02,185	1,02,185
diffutils	3.8	3.8
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugin-support-info	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2
dracut	055	055
dracut-config-ec2	3.0	
dracut-config-generic	055	055
dwz	0,14	0,14
dyninst	102,1	10.2.1
e2fsprogs	1,446,5	1,46,5
e2fsprogs-libs	1,46,5	1,46,5

Pacchetto	AMI	VHDX Hyper-V
ec2-hibinit-agent	1.0.8	
ec2-instance-connect	1.1	
ec 2- instance-connect-selinux	1.1	
ec2-utils	2.2.0	
ed	1.14.2	1.14.2
efi-filesystem	5	5
efi-srpm-macros	5	5
efivar	38	38
efivar-libs	38	38
elfutils-debuginfod-client	0.188	0.188
elfutils-default-yama-scope	0.188	0.188
elfutils-libelf	0.188	0.188
elfutils-libs	0.188	0.188
ethtool	5,15	5,15
expat	2.5.0	2.5.0
file	5,39	5,39
file-libs	5,39	5,39
filesystem	3,14	3,14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5

Pacchetto	AMI	VHDX Hyper-V
fstrm	0.6.1	0.6.1
fuse-libs	2,9,9	29.9
gawk	5.1.0	5.1.0
gdbm-libs	1,19	1,19
gdisk	1.0.8	1.0.8
gettext	0,21	0,21
gettext-libs	0,21	0,21
ghc-srpm-macros	1.5.0	1.5.0
glib2	2,74,7	2,74,7
glibc	2,34	2,34
glibc-all-langpacks	2,34	2,34
glibc-common	2,34	2,34
glibc-gconv-extra	2,34	2,34
glibc-locale-source	2,34	2,34
gmp	62,1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gnutls	3.8.0	3.8.0
go-srpm-macros	3.2.0	3.2.0
gpgme	1.15.1	1.15.1
gpm-libs	1,20.7	1,20.7

Pacchetto	AMI	VHDX Hyper-V
grep	3.8	3.8
groff-base	1,22,4	1,22,4
grub2-common	2,06	2,06
grub2-efi-x64-ec2	2,06	2,06
grub2-pc		2,06
grub2-pc-modules	2,06	2,06
grub2-tools	2,06	2,06
grub2-tools-minimal	2,06	2,06
grubby	8,40	8,40
gssproxy	0.8.4	0.8.4
gzip	1.12	1.12
hostname	3,23	3,23
hunspell	1.7.0	1.7.0
hunspell-en	0,20140811,1	0,20140811,1
hunspell-en-GB	0,20140811,1	0,20140811,1
hunspell-en-US	0,20140811,1	0,20140811,1
hunspell-filesystem	1.7.0	1.7.0
hwdata	0,3353	0,3353
demoni hyperv		0
hyperv-daemons-license		0

Pacchetto	AMI	VHDX Hyper-V
strumenti hyperv		0
hypervfcopyd		0
hypervkvpd		0
hypervvssd		0
Info	6.7	6.7
inih	49	49
initscripts	10,09	10,09
iproute	5.10.0	5.10.0
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0
jansson	2.14	2.14
jitterentropy	3.4.1	3.4.1
jq	1.7.1	1.7.1
json-c	0,14	0,14
kbd	2.4.0	2.4.0
kbd-misc	2.4.0	2.4.0
kernel	61,79	6,1,79
kernel-livepatch-repo-cdn		2023,420240319
kernel-livepatch-repo-s3	2023,420240319	
kernel-modules-extra		6,1,79

Pacchetto	AMI	VHDX Hyper-V
kernel-modules-extra-common		6,1,79
kernel-srpm-macros	1.0	1
kernel-tools	6,1,79	6,1,79
keyutils	1.6.3	1.6.3
keyutils-libs	1.6.3	1.6.3
kmod	29	29
kmod-libs	29	29
kpatch-runtime	0,9,7	0,9,7
krb5-libs	1,21	1,21
less	608	608
libacl	2.3.1	2.3.1
libaio	0,3111	0,3111
libarchive	3,5,3	3,5,3
libargon2	20171227	20171227
libassuan	2,5,5	2,5,5
libattr	2.5.1	2.5.1
libbasicobjects	0,11	01.1
libblkid	2,37,4	2,37,4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2

Pacchetto	AMI	VHDX Hyper-V
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1,446,5	1,46,5
libcomps	01,20	01,20
libconfig	17.2	1.7.2
libcurl-minimal	8,5,0	8,5,0
libdb	5,3,28	5,3,28
libdhash	0,50	
libdnf	0,69,0	0,69,0
libeconf	0,40	0,40
libedit	3.1	3.1
libev	4,33	4,33
libevent	2,1,12	2,1,12
libfdisk	2,37,4	2,37,4
libffi	34.4	34.4
libfido2	1.10.0	1.10.0
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1,42	1,42

Pacchetto	AMI	VHDX Hyper-V
libibverbs	48,0	48,0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmaccalc	1.4.0	1.4.0
libldb	26.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0,13	0,13
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2,37,4	2,37,4
libnfsidmap	2,5,4	2.5.4
libnghttp2	1,57,0	1,57,0
libnl3	3.5.0	3.5.0
libpath_utils	0,2,1	0,2,1
libpcap	1.10.1	1.10.1
libpipeline	1.5.3	1.5.3
libpkgconf	1.8.0	1.8.0
libpsl	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4

Pacchetto	AMI	VHDX Hyper-V
libref_array	0,1,5	0,1,5
librepo	1,14,5	1,14,5
libreport-filesystem	2,15,2	2,15,2
libseccomp	2.5.3	2.5.3
libselinux	3.4	3.4
libselinux-utils	3.4	3.4
libsemanage	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2,13	2,13
libsmartcols	2,37,4	2,37,4
libsolv	0,7,22	0,7,22
libss	1,446,5	1,46,5
libsss_certmap	2,9,4	
libsss_idmap	2,9,4	2,9,4
libsss_nss_idmap	2,9,4	2,9,4
libsss_sudo	2.9.4	
libstdc++	11.4.1	11.4.1
libstoragemgmt	1.9.4	1.9.4
libtalloc	2.3.4	
libtasn1	4,19,0	4,19,0

Pacchetto	AMI	VHDX Hyper-V
libtdb	1.4.7	
libtevent	0.13.0	
libtextstyle	0,21	0,21
libtirpc	1.3.3	1.3.3
libunistring	0,9,10	0,9,10
libuser	0,63	0,63
libutempter	1.2.1	1.2.1
libuuid	2,374	2,37,4
libuv	1.47.0	1.47.0
libverto	0,32	0,32
libverto-libev	0,32	0,32
libxcrypt	4,4,33	4,4,33
libxml2	2,10,4	210.4
libyaml	02,5	02,5
libzstd	1,5,5	1,5,5
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0,9,29	0,9,29
logrotate	3,20,1	3,20,1
lsof	4,94,0	4,94,0
lua-libs	5.4.4	5.4.4

Pacchetto	AMI	VHDX Hyper-V
lua-srpm-macros	1	1
lz4-libs	1.9.4	1.9.4
man-db	2,9,3	29.3
man-pages	5,10	5,10
microcode_ctl	2.1	2.1
mpfr	4.1.0	4.1.0
nano	5.8	5.8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
net-tools	2.0	2.0
nettle	3.8	3.8
newt	0,52,21	0,52,21
nfs-utils	2,5,4	2.5.4
npth	1.6	1.6
nspr	4,35,0	4,35,0
nss	3,90,0	3,90,0
nss-softokn	3,90,0	3,90,0
nss-softokn-freebl	3,90,0	3,90,0
nss-sysinit	3,90,0	3,90,0

Pacchetto	AMI	VHDX Hyper-V
nss-util	3,90,0	3,90,0
ntsysv	1.15	1.15
numactl-libs	2.0,14	2.0,14
ocaml-srpm-macros	6	6
oniguruma	6,9,7,1	6,9,7,1
openblas-srpm-macros	2	2
openldap	2,4,57	2,4,57
openssh	8.7p1	8,7p1
openssh-clients	8,7p1	8,7p1
openssh-server	8,7p1	8,7p1
openssl	3,0,8	30,8
openssl-libs	30,8	30,8
openssl-pkcs11	0,4,12	0,4,12
os-prober	1,77	1,77
p11-kit	0,24,1	0,24,1
p11-kit-trust	0,24,1	0,24,1
package-notes-srpm-macros	0.4	0.4
pam	1.5.1	1.5.1
parted	3.4	3.4
passwd	0,80	0,80

Pacchetto	AMI	VHDX Hyper-V
pciutils	3.7.0	3.7.0
pciutils-libs	3.7.0	3.7.0
pcre2	10,40	10,40
pcre2-syntax	10,40	10,40
perl-Carp	1,50	1,50
perl-Class-Struct	0,66	0,66
perl- DynaLoader	1,47	1,47
perl-Encode	3,15	3,15
perl-Errno	1,30	1,30
perl-Exporter	5,74	5,74
perl-Fcntl	1.13	1.13
perl-File-Basename	2,85	2,85
perl-File-Path	2,18	2,18
perl-File-Temp	0,231,100	0,231,100
perl-File-stat	1,09	1,09
perl-Getopt-Long	2,52	2,52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-IO	1,43	1,43
perl-IPC-Open3	1,21	1,21

Pacchetto	AMI	VHDX Hyper-V
perl-MIME-Base64	3,16	3,16
perl-POSIX	1,94	1,94
perl- PathTools	3,78	3,78
perl-Pod-Escapes	1,07	1,07
perl-Pod-Perldoc	3,28,01	3,28,01
perl-Pod-Simple	3,42	3,42
perl-Pod-Usage	2,01	2,01
perl-Scalar-List-Utils	1,56	1,56
perl- SelectSaver	1.02	1.02
perl-Socket	2.032	2,032
perl-Storable	3,21	3,21
perl-Symbol	1,08	1,08
perl-Term-ANSIColor	5,01	5,01
perl-Term-Cap	1,17	1,17
Testo in Perl- ParseWords	3.30	3,30
perl-Text-Tabs+Wrap	2021,0726	2021,0726
perl-Time-Local	1,300	1.300
perl-constant	1,33	1,33
perl-if	0,60,800	0,60,800
perl-interpreter	5,32,1	5,32,1

Pacchetto	AMI	VHDX Hyper-V
perl-libs	5,32,1	5,32,1
perl-mro	1,23	1,23
perl-overload	1,31	1,31
perl-overloading	0,02	0,02
perl-parent	0,238	0,238
perl-podlators	4,14	4,14
perl-srpm-macros	1	1
perl-subs	1,03	1,03
perl-vars	1,05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4
policycoreutils-python-utils	3.4	
popt	1,18	1,18
procps-ng	3,3,17	3,3,17
protobuf-c	1.4.1	1.4.1
psacct	6,6,4	6.6.4
psmisc	23,4	23,4
publicsuffix-list-dafsa	20240212	20240212

Pacchetto	AMI	VHDX Hyper-V
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
python3	3,9,16	3,9,16
python3-attrs	20,3,0	20,3,0
python3-audit	30.6	3.0.6
python3-awscrt	0,19,19	0,19,19
python3-babel	2,9,1	29.1
python3-cffi	1,14,5	1,14,5
python3-chardet	4.0.0	4.0.0
python3-colorama	04.4	04.4
python3-configobj	50.6	5.0.6
python3-cryptography	36,0	36,0
python3-daemon	2.3.0	
python3-dateutil	28.1	28.1
python3-dbus	1,2,18	1,2,18
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python 3- dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1

Pacchetto	AMI	VHDX Hyper-V
python3-hawkey	0,69,0	0,69,0
python3-idna	(2.10)	(2.10)
python3-jinja2	211,3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1,21	1,21
python3-jsonpointer	2.0	2.0
python3-jsonschema	3.2.0	3.2.0
python3-libcomps	01,20	01,20
python3-libdnf	0,69,0	0,69,0
python3-libs	3,9,16	3,9,16
python3-libselinux	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstoragemgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0,10,6	0,10,6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21,31	21,31
python3-ply	3,11	3,11
python3-policycoreutils	3.4	3.4

Pacchetto	AMI	VHDX Hyper-V
python3-prettytable	0.7.2	0.7.2
python3-prompt-toolkit	3,0,24	3,0,24
python3-pycparser	2,20	2,20
python3-pyrsistent	0,17,3	0,17,3
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022,7,1	2022,7,1
python3-pyyaml	5.4.1	5.4.1
python3-requests	2,25,1	2,25,1
python3-rpm	4,161,3	4,161,3
python3-ruamel-yaml	0,16,6	0,16,6
pitone 3- ruamel-yaml-clib	0.1.2	0,1,2
python3-setools	4.4.1	4.4.1
python3-setuptools	59,60	59,6,0
python3-setuptools-wheel	59,6,0	59,6,0
python3-six	1.15.0	1.15.0
sistema python3	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0,2,5	02,5
quota	4,06	4,06

Pacchetto	AMI	VHDX Hyper-V
quota-nls	4,06	4,06
readline	8.1	8.1
rng-tools	6,14	6,14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4,161,3	4,161,3
rpm-build-libs	4,161,3	4,161,3
rpm-libs	4,161,3	4,161,3
rpm-plugin-selinux	4,161,3	4,161,3
rpm-plugin-systemd-inhibit	4,161,3	4,161,3
rpm-sign-libs	4,161,3	4,161,3
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	37,22	37,22
selinux-policy-targeted	37,22	37,22
setup	2,13,7	2,13,7
shadow-utils	4.9	4.9

Pacchetto	AMI	VHDX Hyper-V
slang	2.3.2	2.3.2
sqlite-libs	3,4,0	3,4,0
sssd-client	2,9,4	2,9,4
sssd-common	2,9,4	
sssd-kcm	2,9,4	
sssd-nfs-idmap	2,9,4	
strace	5,16	5,16
sudo	1,9,14	1,9,14
sysctl-defaults	1.0	1
sysstat	12,5,6	12,5,6
system-release	2023,420240319	2023,420240319
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
systemtap-runtime	4,8	4.8
tar	1,34	1,34
tbb	2020,3	2020,3

Pacchetto	AMI	VHDX Hyper-V
tcpdump	4,99,1	4,99,1
tcsh	6,24,07	6,24,07
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2
userspace-rcu	0.12.1	0.12.1
util-linux	2,37,4	2,37,4
util-linux-core	2,37,4	2,37,4
vim-common	9,0,2153	9,0,2153
vim-data	9,0,2153	9,0,2153
vim-enhanced	9,0,2153	9,0,2153
vim-filesystem	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153
wget	1,21,3	1,21,3
which	2,21	2,21
words	3.0	3.0
xfsdump	3,1,11	3,1,11
xfsprogs	5,18,0	5,18,0

Pacchetto	AMI	VHDX Hyper-V
xxd	9,0,2153	9,0,2153
xxhash-libs	0.8.0	0.8.0
xz	52,5	5.2.5
xz-libs	5.2.5	5.2.5
yum	4.14.0	4.14.0
zip	3.0	3.0
zlib	1,2,11	1,2,11
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	
zstd	1,5,5	1,5,5

Aggiornamento di AL2023

È importante tenersi aggiornati sulle versioni di AL2023 in modo da poter beneficiare degli aggiornamenti di sicurezza e delle nuove funzionalità. Con AL2023, puoi garantire la coerenza tra le versioni e gli aggiornamenti dei pacchetti in tutto l'ambiente tramite Utilizzo degli aggiornamenti deterministici tramite il repository con versioni su AL2023.

Argomenti

Ricevi notifiche sui nuovi aggiornamenti

Puoi ricevere notifiche ogni volta che viene rilasciata una nuova AMI AL2023. Le notifiche vengono pubblicate con Amazon SNS utilizzando il seguente argomento.

```
arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates
```

I messaggi vengono pubblicati qui al momento della pubblicazione di una nuova AMI AL2023. La versione dell'AMI sarà inclusa nel messaggio.

Questi messaggi possono essere ricevuti utilizzando diversi metodi. Ti consigliamo di utilizzare il seguente metodo.

1. Apri la console Amazon SNS.
2. Nella barra di navigazione, modificalo in Stati Uniti orientali (Virginia settentrionale), se necessario. Regione AWS 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 Sottoscrizioni, quindi Crea sottoscrizione.
4. Nella finestra di dialogo Create subscription (Crea sottoscrizione) eseguire le seguenti operazioni:
   a. Per l'argomento ARN, copia e incolla il seguente Amazon Resource Name (ARN):. **`arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates`**

b. Per Protocollo, scegli E-mail.

c. In Endpoint immetti l'indirizzo e-mail utilizzabile per ricevere le notifiche.

d. 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.

Gestione degli aggiornamenti dei pacchetti e del sistema operativo in AL2023

A differenza delle versioni precedenti di Amazon Linux, le AMI AL2023 sono bloccate su una versione specifica del repository Amazon Linux. Per applicare le correzioni di sicurezza e di bug a un'istanza AL2023, aggiorna la configurazione DNF. In alternativa, avvia un'istanza AL2023 più recente.

In questa sezione viene descritto come gestire repository e pacchetti DNF su un'istanza in esecuzione. Viene descritto inoltre come configurare DNF da uno script di dati utente per abilitare il repository Amazon Linux più recente disponibile al momento dell'avvio. Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi DNF.

Argomenti

Verifica degli aggiornamenti dei pacchetti disponibili

Puoi utilizzare il comando `dnf check-update` per verificare la presenza di eventuali aggiornamenti per il sistema. Per AL2023, consigliamo di aggiungere l'opzione `--releasever=`*`version-number`* al comando.

Quando aggiungi questa opzione, DNF verifica anche la presenza di aggiornamenti per una versione successiva del repository. Ad esempio, dopo aver eseguito il comando `dnf check-update`, usa la versione più recente restituita come valore per *`version-number`*.

Se l'istanza viene aggiornata per utilizzare la versione più recente del repository, l'output include un elenco di tutti i pacchetti da aggiornare.

> **Note**
>
> Se non specifichi la versione di rilascio con il flag opzionale al comando `dnf check-update`, viene controllata solo la versione del repository attualmente configurata. Ciò significa che i pacchetti nella versione successiva del repository non vengono controllati.

```
$ sudo dnf check-update --releasever=2023.0.20230210
Last metadata expiration check: 0:06:13 ago on Mon 13 Feb 2023 10:39:32 PM UTC.

bind-libs.x86_64                        32:9.16.27-1.amzn2023          amazonlinux
bind-license.noarch                     32:9.16.27-1.amzn2023          amazonlinux
bind-utils.x86_64                       32:9.16.27-1.amzn2023          amazonlinux
cloud-init.noarch                       22.2.2-1.amzn2023.1.4          amazonlinux
dnf.noarch                              4.12.0-2.amzn2023.0.1          amazonlinux
dnf-data.noarch                         4.12.0-2.amzn2023.0.1          amazonlinux
dracut.x86_64                           055-6.amzn2023.0.4             amazonlinux
dracut-config-generic.x86_64            055-6.amzn2023.0.4             amazonlinux
glib2.x86_64                            2.73.2-678.amzn2023            amazonlinux
gmp.x86_64                              1:6.2.1-2.amzn2023             amazonlinux
grep.x86_64                             3.8-1.amzn2023.0.1             amazonlinux
kpatch-runtime.noarch                   0.9.4-7.amzn2023               amazonlinux
libgcc.x86_64                           11.3.1-2.amzn2023.0.6          amazonlinux
libgomp.x86_64                          11.3.1-2.amzn2023.0.6          amazonlinux
libpkgconf.x86_64                       1.7.3-7.amzn2023.0.1           amazonlinux
libstdc++.x86_64                        11.3.1-2.amzn2023.0.6          amazonlinux
lz4-libs.x86_64                         1.9.4-1.amzn2023               amazonlinux
pkgconf.x86_64                          1.7.3-7.amzn2023.0.1           amazonlinux
pkgconf-m4.noarch                       1.7.3-7.amzn2023.0.1           amazonlinux
pkgconf-pkg-config.x86_64               1.7.3-7.amzn2023.0.1           amazonlinux
python3-dnf.noarch                      4.12.0-2.amzn2023.0.1          amazonlinux
python3-rpm.x86_64                      4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm.x86_64                              4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-build-libs.x86_64                   4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-libs.x86_64                         4.16.1.3-12.amzn2023.0.2       amazonlinux
```

```
rpm-plugin-selinux.x86_64             4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-plugin-systemd-inhibit.x86_64     4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-sign-libs.x86_64                  4.16.1.3-12.amzn2023.0.2       amazonlinux
slang.x86_64                          2.3.2-9.amzn2023.0.1           amazonlinux
system-release.noarch                 2023.0.20230210-0.amzn2023     amazonlinux
systemd.x86_64                        250.8-1.amzn2023.0.1           amazonlinux
systemd-libs.x86_64                   250.8-1.amzn2023.0.1           amazonlinux
systemd-networkd.x86_64               250.8-1.amzn2023.0.1           amazonlinux
systemd-pam.x86_64                    250.8-1.amzn2023.0.1           amazonlinux
systemd-resolved.x86_64               250.8-1.amzn2023.0.1           amazonlinux
systemd-udev.x86_64                   250.8-1.amzn2023.0.1           amazonlinux
vim-common.x86_64                     2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-data.noarch                       2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-enhanced.x86_64                   2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-filesystem.noarch                 2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-minimal.x86_64                    2:9.0.327-1.amzn2023.0.1       amazonlinux
wget.x86_64                           1.21.3-1.amzn2023              amazonlinux
yum.noarch                            4.12.0-2.amzn2023.0.1          amazonlinux
```

Per questo comando, se sono disponibili pacchetti più recenti, il codice restituito è 100. Se non sono disponibili pacchetti più recenti, il codice restituito è 0. Inoltre, l'output elenca anche tutti i pacchetti da aggiornare.

Applicazione degli aggiornamenti di sicurezza utilizzando DNF e le versioni del repository

I nuovi aggiornamenti dei pacchetti e gli aggiornamenti di sicurezza sono disponibili solo per le nuove versioni del repository. Per le istanze avviate da versioni delle AMI AL2023 precedenti, devi aggiornare la versione del repository prima di poter installare gli aggiornamenti di sicurezza. Il comando `dnf check-release-update` include un comando di aggiornamento di esempio che aggiorna tutti i pacchetti installati sul sistema alle versioni in un repository più recente.

```
$ sudo dnf update --releasever=2023.0.20230210
Last metadata expiration check: 0:01:40 ago on Mon 13 Feb 2023 10:39:32 PM UTC.
Dependencies resolved.
================================================================================
 Package                    Arch   Version                    Repository   Size
================================================================================
Upgrading:
 bind-libs                  x86_64 32:9.16.27-1.amzn2023      amazonlinux 1.2 M
 bind-license               noarch 32:9.16.27-1.amzn2023      amazonlinux  16 k
```

```
 bind-utils                  x86_64 32:9.16.27-1.amzn2023      amazonlinux 202 k
 cloud-init                  noarch 22.2.2-1.amzn2023.1.4      amazonlinux 1.1 M
 dnf                         noarch 4.12.0-2.amzn2023.0.1      amazonlinux 454 k
 dnf-data                    noarch 4.12.0-2.amzn2023.0.1      amazonlinux  42 k
 dracut                      x86_64 055-6.amzn2023.0.4         amazonlinux 345 k
 dracut-config-generic       x86_64 055-6.amzn2023.0.4         amazonlinux 8.5 k
 glib2                       x86_64 2.73.2-678.amzn2023        amazonlinux 2.7 M
 gmp                         x86_64 1:6.2.1-2.amzn2023         amazonlinux 324 k
 grep                        x86_64 3.8-1.amzn2023.0.1         amazonlinux 316 k
 kpatch-runtime              noarch 0.9.4-7.amzn2023           amazonlinux  30 k
 libgcc                      x86_64 11.3.1-2.amzn2023.0.6      amazonlinux 121 k
 libgomp                     x86_64 11.3.1-2.amzn2023.0.6      amazonlinux 296 k
 libpkgconf                  x86_64 1.7.3-7.amzn2023.0.1       amazonlinux  37 k
 libstdc++                   x86_64 11.3.1-2.amzn2023.0.6      amazonlinux 758 k
 lz4-libs                    x86_64 1.9.4-1.amzn2023           amazonlinux  81 k
 pkgconf                     x86_64 1.7.3-7.amzn2023.0.1       amazonlinux  41 k
 pkgconf-m4                  noarch 1.7.3-7.amzn2023.0.1       amazonlinux  15 k
 pkgconf-pkg-config          x86_64 1.7.3-7.amzn2023.0.1       amazonlinux  11 k
 python3-dnf                 noarch 4.12.0-2.amzn2023.0.1      amazonlinux 415 k
 python3-rpm                 x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  89 k
 rpm                         x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux 487 k
 rpm-build-libs              x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  92 k
 rpm-libs                    x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux 311 k
 rpm-plugin-selinux          x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  18 k
 rpm-plugin-systemd-inhibit x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  19 k
 rpm-sign-libs               x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  22 k
 slang                       x86_64 2.3.2-9.amzn2023.0.1       amazonlinux 410 k
 system-release              noarch 2023.0.20230210-0.amzn2023 amazonlinux  25 k
 systemd                     x86_64 250.8-1.amzn2023.0.1       amazonlinux 4.2 M
 systemd-libs                x86_64 250.8-1.amzn2023.0.1       amazonlinux 615 k
 systemd-networkd            x86_64 250.8-1.amzn2023.0.1       amazonlinux 614 k
 systemd-pam                 x86_64 250.8-1.amzn2023.0.1       amazonlinux 335 k
 systemd-resolved            x86_64 250.8-1.amzn2023.0.1       amazonlinux 277 k
 systemd-udev                x86_64 250.8-1.amzn2023.0.1       amazonlinux 1.9 M
 vim-common                  x86_64 2:9.0.327-1.amzn2023.0.1   amazonlinux 7.2 M
 vim-data                    noarch 2:9.0.327-1.amzn2023.0.1   amazonlinux  27 k
 vim-enhanced                x86_64 2:9.0.327-1.amzn2023.0.1   amazonlinux 1.8 M
 vim-filesystem              noarch 2:9.0.327-1.amzn2023.0.1   amazonlinux  21 k
 vim-minimal                 x86_64 2:9.0.327-1.amzn2023.0.1   amazonlinux 764 k
 wget                        x86_64 1.21.3-1.amzn2023          amazonlinux 813 k
 yum                         noarch 4.12.0-2.amzn2023.0.1      amazonlinux  39 k

Transaction Summary
================================================================================
```

```
Upgrade  43 Packages
...
```

Puoi aggiungere l'opzione `--security` per aggiornare i pacchetti solo con le funzionalità di sicurezza.

```
$ sudo dnf update --releasever=2023.0.20230210 --security
Amazon Linux 2023 repository                    18 MB/s |  11 MB     00:00
Last metadata expiration check: 0:00:02 ago on Mon 13 Feb 2023 10:39:32 PM UTC.
Dependencies resolved.
================================================================================
 Package           Arch      Version                         Repository      Size
================================================================================
Upgrading:
 bind-libs         x86_64    32:9.16.27-1.amzn2023           amazonlinux    1.2 M
 bind-license      noarch    32:9.16.27-1.amzn2023           amazonlinux     16 k
 bind-utils        x86_64    32:9.16.27-1.amzn2023           amazonlinux    202 k
 gmp               x86_64    1:6.2.1-2.amzn2023              amazonlinux    324 k
 lz4-libs          x86_64    1.9.4-1.amzn2023                amazonlinux     81 k
 vim-common        x86_64    2:9.0.327-1.amzn2023.0.1        amazonlinux    7.2 M
 vim-data          noarch    2:9.0.327-1.amzn2023.0.1        amazonlinux     27 k
 vim-enhanced      x86_64    2:9.0.327-1.amzn2023.0.1        amazonlinux    1.8 M
 vim-filesystem    noarch    2:9.0.327-1.amzn2023.0.1        amazonlinux     21 k
 vim-minimal       x86_64    2:9.0.327-1.amzn2023.0.1        amazonlinux    764 k
 wget              x86_64    1.21.3-1.amzn2023               amazonlinux    813 k

Transaction Summary
================================================================================
Upgrade  11 Packages
...
```

Per scoprire le versioni dei pacchetti di AL2023, esegui una o più delle seguenti operazioni:

- Esegui il comando `dnf check-update`.
- Sottoscrivi l'argomento SNS per l'aggiornamento del repository Amazon Linux (`arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates`). Per ulteriori informazioni, consulta Sottoscrizione a un argomento di Amazon SNS nella Guida per lo Sviluppatore di Amazon Simple Notification Service.
- Consulta regolarmente le note di rilascio di AL2023.

> **Important**
>
> Quando applichi aggiornamenti di sicurezza a un'istanza in esecuzione, assicurati che DNF punti alla versione più recente del repository.

Riavvio automatico del servizio dopo gli aggiornamenti (di sicurezza)

Amazon Linux ora viene fornito con il pacchetto smart-restart. `Smart-restart`riavvia i servizi systemd sugli aggiornamenti di sistema ogni volta che un pacchetto viene installato o eliminato utilizzando il gestore di pacchetti del sistema. Ciò si verifica ogni volta che `dnf (update|upgrade|downgrade)` viene eseguito.

`Smart-restart`utilizza il `needs-restarting` pacchetto from `dnf-utils` e un meccanismo di denylisting personalizzato per determinare quali servizi devono essere riavviati e se è consigliato il riavvio del sistema. Se si consiglia il riavvio del sistema, viene generato un file marker di suggerimento per il riavvio (). `/run/smart-restart/reboot-hint-marker`

Per installare **`smart-restart`**

Eseguite il DNF comando seguente (come fareste con qualsiasi altro pacchetto).

```
$ sudo dnf install smart-restart
```

Dopo l'installazione, le transazioni successive attiveranno la `smart-restart` logica.

Lista di rifiuto

`Smart-restart`può essere richiesto di bloccare il riavvio di determinati servizi. I servizi bloccati non contribuiranno alla decisione se è necessario un riavvio. Per bloccare servizi aggiuntivi, aggiungete un file con il suffisso `-denylist` in, `/etc/smart-restart-conf.d/` come illustrato nell'esempio seguente.

```
$ cat /etc/smart-restart-conf.d/custom-denylist
# Some comments
myservice.service
```

> **Note**
>
> Tutti `*-denylist` i file vengono letti e valutati quando si decide se è necessario un riavvio.

Ganci personalizzati

Oltre al denylisting, `smart-restart` fornisce un meccanismo per eseguire script personalizzati prima e dopo i tentativi di riavvio del servizio. Gli script personalizzati possono essere utilizzati per eseguire manualmente le fasi di preparazione o per informare gli altri componenti del riavvio residuo o completato.

Tutti gli script vengono inseriti `/etc/smart-restart-conf.d/` con il suffisso `-pre-restart` o `-post-restart` vengono eseguiti. Se l'ordine è importante, aggiungete un numero a tutti gli script per garantire l'ordine di esecuzione, come illustrato nell'esempio seguente.

```
$ ls /etc/smart-restart-conf.d/*-pre-restart
001-my-script-pre-restart
002-some-other-script-pre-restart
```

Avvio di un'istanza con la versione più recente del repository abilitata

Puoi aggiungere comandi DNF a uno script di dati utente per controllare quali pacchetti RPM vengono installati su un'AMI Amazon Linux al momento dell'avvio. Nell'esempio seguente, viene utilizzato uno script di dati utente per assicurarsi che su ogni istanza avviata con lo script di dati utente siano installati gli stessi aggiornamenti del pacchetto.

```
#!/bin/bash
dnf update --releasever=2023.0.20230210
# Additional setup and install commands below
dnf install httpd php7.4 mysql80
```

È necessario eseguire questo script come utente con privilegi avanzati (root). Per farlo, esegui il comando seguente.

```
$ sudo sh -c "bash nameofscript.sh"
```

Per ulteriori informazioni, consulta la pagina dedicata agli script di dati utente e shell nella Guida per l'utente di Amazon EC2 per le istanze Linux.

> **Note**
>
> Invece di utilizzare uno script di dati utente, avvia l'AMI Amazon Linux più recente o un'AMI personalizzata basata sull'AMI Amazon Linux. L'AMI Amazon Linux più recente dispone di tutti gli aggiornamenti necessari installati ed è configurata in modo che punti a una particolare versione del repository.

Ottenere informazioni di supporto per i pacchetti

AL2023 incorpora molti diversi progetti software open source. Ciascuno di questi progetti è gestito indipendentemente da Amazon Linux e prevede release e end-of-support pianificazioni diverse. Per fornirti informazioni specifiche su Amazon Linux in relazione a questi diversi pacchetti, il plugin `supportinfo` DNF fornisce i metadati relativi a un pacchetto. Nell'esempio seguente, il comando **`dnf supportinfo`** restituisce i metadati per il pacchetto `glibc`.

```
$ sudo dnf supportinfo --pkg glibc
Last metadata expiration check: 0:07:56 ago on Wed Mar  1 23:21:49 2023.
Name                 : glibc
Version              : 2.34-52.amzn2023.0.2
State                : installed
Support Status       : supported
Support Periods      : from 2023-03-15      : supported
                     : from 2028-03-15      : unsupported
Support Statement    : Amazon Linux 2023 End Of Life
Link                 : https://aws.amazon.com/amazon-linux-ami/faqs/
Other Info           : This is the support statement for AL2023. The
     ...: end of life of Amazon Linux 2023 would be March 2028.
     ...: From this point, the Amazon Linux 2023 packages (listed
     ...: below) will no longer, receive any updates from AWS.
```

Verifica della disponibilità di versioni più recenti del repository

In un'istanza AL2023, puoi usare l'utilità DNF per gestire i repository e applicare pacchetti RPM aggiornati. Questi pacchetti sono disponibili nei repository Amazon Linux. Puoi usare il comando DNF `dnf check-release-update` per verificare la presenza di nuove versioni del repository DNF.

```
$ sudo dnf check-release-update
WARNING:
  A newer release of "Amazon Linux" is available.
```

```
  Available Versions:

  Version 2023.0.20230210:
    Run the following command to update to 2023.0.20230210:

      dnf update --releasever=2023.0.20230210

    Release notes:
     https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes.html
```

Questa operazione restituisce un elenco completo di tutte le versioni più recenti dei repository DNF disponibili. Se non viene restituito nulla, significa che DNF è attualmente configurato per utilizzare la versione più recente disponibile. La versione del pacchetto `system-release` attualmente installata imposta la variabile `releasever` DNF. Per controllare la versione attuale del repository, esegui il comando seguente.

```
$ rpm -q system-release --qf "%{VERSION}\n"
```

Quando si eseguono transazioni di pacchetti DNF (ad esempio comandi di installazione, aggiornamento o rimozione), un messaggio di avviso segnala eventuali nuove versioni del repository. Ad esempio, se installi il pacchetto `httpd` su un'istanza avviata da una versione precedente di AL2023, viene restituito il seguente output.

```
$ sudo dnf install httpd -y
Last metadata expiration check: 0:16:52 ago on Wed Mar  1 23:21:49 2023.
Dependencies resolved.
================================================================================
 Package            Arch   Version                Repository   Size
================================================================================
Installing:
 httpd              x86_64 2.4.54-3.amzn2023.0.4  amazonlinux  46 k
Installing dependencies:
 apr                x86_64 1.7.2-2.amzn2023.0.2   amazonlinux 129 k
 apr-util           x86_64 1.6.3-1.amzn2023.0.1   amazonlinux  98 k
 generic-logos-httpd
                    noarch 18.0.0-12.amzn2023.0.3 amazonlinux  19 k
 httpd-core         x86_64 2.4.54-3.amzn2023.0.4  amazonlinux 1.3 M
 httpd-filesystem   noarch 2.4.54-3.amzn2023.0.4  amazonlinux  13 k
 httpd-tools        x86_64 2.4.54-3.amzn2023.0.4  amazonlinux  80 k
 libbrotli          x86_64 1.0.9-4.amzn2023.0.2   amazonlinux 315 k
```

```
 mailcap            noarch 2.1.49-3.amzn2023.0.3  amazonlinux  33 k
Installing weak dependencies:
 apr-util-openssl   x86_64 1.6.3-1.amzn2023.0.1   amazonlinux  17 k
 mod_http2          x86_64 1.15.24-1.amzn2023.0.3 amazonlinux 152 k
 mod_lua            x86_64 2.4.54-3.amzn2023.0.4  amazonlinux  60 k

Transaction Summary
================================================================================
Install  12 Packages

Total download size: 2.3 M
Installed size: 6.8 M
Downloading Packages:
(1/12): apr-util-openssl-1.6.3-1.am 212 kB/s |  17 kB     00:00
(2/12): apr-1.7.2-2.amzn2023.0.2.x8 1.1 MB/s | 129 kB     00:00
(3/12): httpd-core-2.4.54-3.amzn202 8.9 MB/s | 1.3 MB     00:00
(4/12): mod_http2-1.15.24-1.amzn202 1.9 MB/s | 152 kB     00:00
(5/12): apr-util-1.6.3-1.amzn2023.0 1.7 MB/s |  98 kB     00:00
(6/12): mod_lua-2.4.54-3.amzn2023.0 1.4 MB/s |  60 kB     00:00
(7/12): httpd-2.4.54-3.amzn2023.0.4 1.5 MB/s |  46 kB     00:00
(8/12): libbrotli-1.0.9-4.amzn2023. 4.4 MB/s | 315 kB     00:00
(9/12): mailcap-2.1.49-3.amzn2023.0 753 kB/s |  33 kB     00:00
(10/12): httpd-tools-2.4.54-3.amzn2 978 kB/s |  80 kB     00:00
(11/12): httpd-filesystem-2.4.54-3. 210 kB/s |  13 kB     00:00
(12/12): generic-logos-httpd-18.0.0 439 kB/s |  19 kB     00:00
--------------------------------------------------------------------------------
Total                               6.6 MB/s | 2.3 MB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : apr-1.7.2-2.amzn2023.0.2.x86_64                        1/12
  Installing       : apr-util-openssl-1.6.3-1.amzn2023.0.1.                 2/12
  Installing       : apr-util-1.6.3-1.amzn2023.0.1.x86_64                   3/12
  Installing       : mailcap-2.1.49-3.amzn2023.0.3.noarch                   4/12
  Installing       : httpd-tools-2.4.54-3.amzn2023.0.4.x86_                 5/12
  Installing       : generic-logos-httpd-18.0.0-12.amzn2023                 6/12
  Running scriptlet: httpd-filesystem-2.4.54-3.amzn2023.0.4                 7/12
  Installing       : httpd-filesystem-2.4.54-3.amzn2023.0.4                 7/12
  Installing       : httpd-core-2.4.54-3.amzn2023.0.4.x86_6                 8/12
  Installing       : mod_http2-1.15.24-1.amzn2023.0.3.x86_6                 9/12
  Installing       : libbrotli-1.0.9-4.amzn2023.0.2.x86_64                 10/12
```

```
  Installing       : mod_lua-2.4.54-3.amzn2023.0.4.x86_64     11/12
  Installing       : httpd-2.4.54-3.amzn2023.0.4.x86_64       12/12
  Running scriptlet: httpd-2.4.54-3.amzn2023.0.4.x86_64       12/12
  Verifying        : apr-1.7.2-2.amzn2023.0.2.x86_64           1/12
  Verifying        : apr-util-openssl-1.6.3-1.amzn2023.0.1.    2/12
  Verifying        : httpd-core-2.4.54-3.amzn2023.0.4.x86_6    3/12
  Verifying        : mod_http2-1.15.24-1.amzn2023.0.3.x86_6    4/12
  Verifying        : apr-util-1.6.3-1.amzn2023.0.1.x86_64      5/12
  Verifying        : mod_lua-2.4.54-3.amzn2023.0.4.x86_64      6/12
  Verifying        : libbrotli-1.0.9-4.amzn2023.0.2.x86_64     7/12
  Verifying        : httpd-2.4.54-3.amzn2023.0.4.x86_64        8/12
  Verifying        : httpd-tools-2.4.54-3.amzn2023.0.4.x86_    9/12
  Verifying        : mailcap-2.1.49-3.amzn2023.0.3.noarch     10/12
  Verifying        : httpd-filesystem-2.4.54-3.amzn2023.0.4   11/12
  Verifying        : generic-logos-httpd-18.0.0-12.amzn2023   12/12

Installed:
  apr-1.7.2-2.amzn2023.0.2.x86_64
  apr-util-1.6.3-1.amzn2023.0.1.x86_64
  apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
  generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
  httpd-2.4.54-3.amzn2023.0.4.x86_64
  httpd-core-2.4.54-3.amzn2023.0.4.x86_64
  httpd-filesystem-2.4.54-3.amzn2023.0.4.noarch
  httpd-tools-2.4.54-3.amzn2023.0.4.x86_64
  libbrotli-1.0.9-4.amzn2023.0.2.x86_64
  mailcap-2.1.49-3.amzn2023.0.3.noarch
  mod_http2-1.15.24-1.amzn2023.0.3.x86_64
  mod_lua-2.4.54-3.amzn2023.0.4.x86_64

Complete!
```

Aggiunta, abilitazione o disabilitazione di nuovi repository

Per installare un pacchetto da un repository diverso con il sistema di gestione dei pacchetti DNF, aggiungi le informazioni relative al repository nel file `/etc/dnf/dnf.conf` o nel relativo file *`repository.repo`* all'interno della directory `/etc/yum.repos.d`. Questa operazione può essere eseguita manualmente. Tuttavia, per la maggior parte dei repository DNF è disponibile il relativo file *`repository.repo`* nell'URL del repository corrispondente.

> **Note**
>
> Al momento, non ci sono altri repository che possono essere aggiunti ad AL2023. Ciò potrebbe cambiare in futuro. Inoltre, puoi scrivere pacchetti personalizzati e renderli disponibili per l'ambiente aziendale AL2023. Prima di poter utilizzare i pacchetti, devi aggiungere e abilitare il repository in cui sono archiviati i pacchetti.

Per scoprire quali repository sono attualmente abilitati, puoi eseguire il seguente comando:

```
$ dnf repolist all --verbose
Loaded plugins: builddep, changelog, config-manager, copr, debug, debuginfo-install,
 download, generate_completion_cache, groups-manager, needs-restarting, playground,
 release-notification, repoclosure, repodiff, repograph, repomanage, reposync,
 supportinfo
DNF version: 4.12.0
cachedir: /var/cache/dnf
Last metadata expiration check: 0:00:02 ago on Wed Mar  1 23:40:15 2023.
Repo-id            : amazonlinux
Repo-name          : Amazon Linux 2023 repository
Repo-status        : enabled
Repo-revision      : 1677203368
Repo-updated       : Fri Feb 24 01:49:28 2023
Repo-pkgs          : 12632
Repo-available-pkgs: 12632
Repo-size          : 12 G
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/mirrors/2023.0.20230222/x86_64/mirror.list
Repo-baseurl       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/guids/
cf9296325a6c46ff40c775a8e2d632c4c3fd9d9164014ce3304715d61b90ca8e/x86_64/
                   : (0 more)
Repo-expire        : 172800 second(s) (last: Wed Mar  1 23:40:15
                   : 2023)
Repo-filename      : /etc/yum.repos.d/amazonlinux.repo

Repo-id            : amazonlinux-debuginfo
Repo-name          : Amazon Linux 2023 repository - Debug
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/mirrors/2023.0.20230222/debuginfo/x86_64/mirror.list
Repo-expire        : 21600 second(s) (last: unknown)
```

```
Repo-filename      : /etc/yum.repos.d/amazonlinux.repo

Repo-id            : amazonlinux-source
Repo-name          : Amazon Linux 2023 repository - Source packages
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/mirrors/2023.0.20230222/SRPMS/mirror.list
Repo-expire        : 21600 second(s) (last: unknown)
Repo-filename      : /etc/yum.repos.d/amazonlinux.repo

Repo-id            : kernel-livepatch
Repo-name          : Amazon Linux 2023 Kernel Livepatch repository
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/kernel-livepatch/mirrors/al2023/x86_64/mirror.list
Repo-expire        : 172800 second(s) (last: unknown)
Repo-filename      : /etc/yum.repos.d/kernel-livepatch.repo

Repo-id            : kernel-livepatch-source
Repo-name          : Amazon Linux 2023 Kernel Livepatch repository -
                   : Source packages
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/kernel-livepatch/mirrors/al2023/SRPMS/mirror.list
Repo-expire        : 21600 second(s) (last: unknown)
Repo-filename      : /etc/yum.repos.d/kernel-livepatch.repo
Total packages: 12632
```

> **Note**
>
> Se non aggiungi il flag di opzione `--verbose`, l'output include solo le informazioni `Repo-id`, `Repo-name` e `Repo-status`.

Per aggiungere un repository **`yum`** alla directory **`/etc/yum.repos.d`**:

1. Cerca la posizione del file `.repo`. In questo esempio, il file `.repo` è disponibile in *`https://www.example.com/repository.repo`*.
2. Aggiungi il repository con il comando `dnf config-manager`.

```
$ sudo dnf config-manager --add-repo https://www.example.com/repository.repo
```

```
Loaded plugins: priorities, update-motd, upgrade-helper
adding repo from: https://www.example.com/repository.repo
grabbing file https://www.example.com/repository.repo to /etc/
yum.repos.d/repository.repo
repository.repo                                          | 4.0 kB     00:00
repo saved to /etc/yum.repos.d/repository.repo
```

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

Per abilitare un repository yum in `/etc/yum.repos.d`, usa il comando `dnf config-manager` con il flag `--enable` e il nome del *repository*.

```
$ sudo dnf config-manager --enable repository
```

> **Note**
>
> Per disabilitare un repository, usa la stessa sintassi del comando, ma sostituendo `--enable` con `--disable` nel comando.

Aggiunta di repository con cloud-init

Oltre ad aggiungere un repository utilizzando il precedente metodo, puoi anche aggiungere un nuovo repository utilizzando il framework `cloud-init`.

Per aggiungere un nuovo repository di pacchetti, si consiglia l'uso del seguente modello. Valuta la possibilità di salvare il file in locale.

```
#cloud-config
yum_repos:
  repository.repo:
    baseurl: https://www.example.com/
    enabled: true
    gpgcheck: true
    gpgkey: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EXAMPLE
    name: Example Repository
```

> **Note**
>
> Un vantaggio dell'utilizzo di `cloud-init` consiste nella possibilità di aggiungere una sezione `packages:` al file di configurazione. In questa sezione, puoi includere i nomi dei pacchetti che desideri installare. Puoi installare i pacchetti dal repository predefinito o dal nuovo repository aggiunto nel file `cloud-config`.
> Per informazioni più specifiche sulla struttura del file YAML, consulta la pagina dedicata all'aggiunta di un repository YUM nella documentazione di *`cloud-init`*.

Dopo aver configurato il file in formato YAML, puoi eseguirlo nel framework `cloud-init` nell'interfaccia AWS CLI. Assicurati di includere l'opzione `--userdata` e il nome del file `.yml` per chiamare le operazioni desiderate.

```
$ aws ec2 run-instances \
  --image-id \
    resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
  --instance-type m5.xlarge \
  --region us-east-1 \
  --key-name aws-key-us-east-1 \
  --security-group-ids sg-004a7650 \
  --user-data file://cloud-config.yml
```

Utilizzo degli aggiornamenti deterministici tramite il repository con versioni su AL2023

> **Note**
>
> Per impostazione predefinita, l'istanza AL2023 non riceve automaticamente aggiornamenti di sicurezza critici e importanti aggiuntivi al momento dell'avvio. Le istanze contengono inizialmente gli aggiornamenti disponibili nella versione di AL2023 e l'AMI scelta.

Controllo degli aggiornamenti ricevuti dai rilasci principali e secondari

Con AL2023, puoi garantire la coerenza tra le versioni e gli aggiornamenti dei pacchetti in tutto l'ambiente. Puoi anche garantire la coerenza per più istanze della stessa Amazon Machine Image

(AMI). Con la funzionalità degli aggiornamenti deterministici tramite repository con controllo delle versioni di AL2023, attivata per impostazione predefinita, puoi applicare gli aggiornamenti in base a una pianificazione che soddisfi le tue esigenze specifiche.

Ogni volta che rilasciamo nuovi aggiornamenti per i pacchetti, ci sono una nuova versione da applicare e nuove AMI che si collegano a quella versione.

AL2023 si collega a una versione specifica del repository. Questa funzionalità è supportata sia per le versioni principali che per quelle secondarie. L'AMI AL2023, esposta tramite i nostri parametri SSM, è sempre la versione più recente. Contiene il maggior numero di up-to-date pacchetti e aggiornamenti, inclusi aggiornamenti di sicurezza critici e importanti.

Se avvii un'istanza da un'AMI esistente, gli aggiornamenti non vengono applicati automaticamente. Tutti i pacchetti aggiuntivi installati come parte del provisioning vengono mappati alla versione del repository dell'AMI esistente.

Con questa funzionalità, hai la responsabilità di garantire la coerenza tra le versioni dei pacchetti e degli aggiornamenti in tutto l'ambiente. Questo è particolarmente vero se stai avviando più istanze dalla stessa AMI. Puoi applicare gli aggiornamenti in base a una pianificazione in grado di soddisfare le tue esigenze. Puoi anche applicare un set specifico di aggiornamenti al momento dell'avvio, poiché questi possono anche essere collegati a una versione specifica del repository.

Differenze tra aggiornamenti delle versioni principali e secondarie

Le versioni principali di AL2023 includono aggiornamenti su larga scala e potrebbero aggiungere, eliminare o aggiornare i pacchetti. Per garantire la compatibilità, aggiorna l'istanza a una nuova versione principale solo dopo aver testato l'applicazione su tale versione.

Le versioni secondarie di AL2023 includono aggiornamenti di funzionalità e sicurezza, ma non includono modifiche ai pacchetti. Ciò garantisce che le funzionalità di Linux e l'API della libreria di sistema rimangano disponibili nelle nuove versioni. Non è necessario testare l'applicazione prima dell'aggiornamento.

Controlla gli aggiornamenti dei pacchetti disponibili dai repository AL2023

Quando pubblichiamo una nuova versione dei repository AL2023, tutte le versioni precedenti sono ancora disponibili. Per impostazione predefinita, il plug-in per la gestione delle versioni dei repository si collega alla stessa versione utilizzata per sviluppare l'AMI. Se desideri controllare gli aggiornamenti dei pacchetti, procedi come segue.

1. Scopri le versioni dei repository disponibili eseguendo il comando riportato di seguito.

```
$ sudo dnf check-release-update
```

2. Seleziona una versione eseguendo il comando seguente.

```
$ sudo dnf --releasever=version update
```

Questo comando avvia un aggiornamento utilizzando `dnf` dalla versione di rilascio attuale di Amazon Linux alla versione di rilascio specificata nella riga di comando. Un elenco degli aggiornamenti dei pacchetti è presentato da `dnf`. Prima di elaborare l'aggiornamento, devi confermarlo. Una volta completato l'aggiornamento, la nuova versione di rilascio diventa la versione di rilascio predefinita che `dnf` usa per tutte le attività future.

Per ulteriori informazioni, consulta Gestione degli aggiornamenti dei pacchetti e del sistema operativo in AL2023.

Aggiornamenti deterministici tramite utilizzo di repository con versioni

Argomenti

- Uso di un sistema di aggiornamento deterministico
- Aggiornamento selettivo di un sistema con aggiornamento deterministico
- Uso dell'override persistente con aggiornamento deterministico

Uso di un sistema di aggiornamento deterministico

Quando esegui il comando `dnf upgrade`, il sistema verifica la presenza di aggiornamenti nel repository specificato dalla variabile `releasever`. *`Una versione valida releasever è l'ultima o una versione con data, ad esempio 2023.3.20240219.`*

È possibile modificare il valore di `releasever` utilizzando uno dei metodi descritti di seguito. Questi metodi sono elencati con priorità di sistema decrescente. Ciò significa che il metodo 1 sostituisce i metodi 2 e 3, e il metodo 2 sostituisce il metodo 3.

1. Il valore nel flag della riga di comando, `--releasever=`*`latest`*, se utilizzato.
2. Il valore specificato nel file della variabile di override, `/etc/dnf/vars/releasever`, se impostato.

3. La versione attualmente installata del pacchetto `system-release`.

Nell'esempio seguente, la versione è *2023.0.20230210*:

```
$ rpm -q system-release
system-release-2023.0.20230210-0.amzn2023.noarch
```

In un sistema appena installato, la variabile di override non è presente. Non sono disponibili aggiornamenti perché il sistema è bloccato sulla versione installata di `system-release`.

```
$ cat /etc/dnf/vars/releasever
cat: /etc/dnf/vars/releasever: No such file or directory
```

```
$ sudo dnf upgrade
Last metadata expiration check: 0:00:02 ago on Wed 15 Feb 2023 06:14:12 PM UTC.
Dependencies resolved.
Nothing to do.
Complete!
```

Puoi ottenere pacchetti di una versione specifica utilizzando il flag `releasever` per fornire la versione desiderata.

```
$ rpm -q system-release
system-release-2023.0.20230222-0.amzn2023.noarch
```

```
$ sudo dnf upgrade --releasever=2023.0.20230329
Amazon Linux 2023 repository                    26 MB/s |  12 MB     00:00
Dependencies resolved.
================================================================================
 Package                 Arch    Version                      Repository   Size
================================================================================
Installing:
 kernel                  aarch64 6.1.21-1.45.amzn2023         amazonlinux  26 M
Upgrading:
 amazon-linux-repo-s3    noarch  2023.0.20230329-0.amzn2023   amazonlinux  18 k
 ca-certificates         noarch  2023.2.60-1.0.amzn2023.0.1   amazonlinux 828 k
 cloud-init              noarch  22.2.2-1.amzn2023.1.7        amazonlinux 1.1 M

         ... [ list edited for clarity ]
```

```
 system-release           noarch  2023.0.20230329-0.amzn2023  amazonlinux  29 k

         ... [ list edited for clarity ]

 vim-data                 noarch  2:9.0.1403-1.amzn2023.0.1   amazonlinux  25 k
 vim-minimal              aarch64 2:9.0.1403-1.amzn2023.0.1   amazonlinux 753 k

Transaction Summary
================================================================================
Install    1 Package
Upgrade   42 Packages

Total download size: 56 M
```

Poiché l'opzione `--releasever` sostituisce sia `system-release` che `/etc/dnf/vars/releasever`, il risultato di questo aggiornamento è il seguente:

1. L'aggiornamento sostituisce tutti i pacchetti installati che sono stati modificati tra la versione precedente e quella nuova.
2. L'aggiornamento blocca il sistema nel repository per la nuova versione di `system-release`.

Aggiornamento selettivo di un sistema con aggiornamento deterministico

Potresti voler installare pacchetti selezionati da un rilascio recente, lasciando al contempo il sistema bloccato sulla versione di rilascio originale.

Puoi utilizzare `dnf check-update` per identificare i pacchetti di cui vuoi eseguire l'aggiornamento.

```
$ sudo dnf check-update --releasever=latest --security
Amazon Linux 2023 repository                    13 MB/s |  10 MB     00:00
Last metadata expiration check: 0:00:02 ago on Wed 15 Feb 2023 02:52:21 AM UTC.

bind-libs.aarch64                 32:9.16.27-1.amzn2023.0.1         amazonlinux
bind-license.noarch               32:9.16.27-1.amzn2023.0.1         amazonlinux
bind-utils.aarch64                32:9.16.27-1.amzn2023.0.1         amazonlinux
cryptsetup.aarch64                2.4.3-2.amzn2023.0.1              amazonlinux
cryptsetup-libs.aarch64           2.4.3-2.amzn2023.0.1              amazonlinux
curl-minimal.aarch64              7.85.0-1.amzn2023.0.1             amazonlinux
glibc.aarch64                     2.34-40.amzn2023.0.2              amazonlinux
glibc-all-langpacks.aarch64       2.34-40.amzn2023.0.2              amazonlinux
glibc-common.aarch64              2.34-40.amzn2023.0.2              amazonlinux
```

```
glibc-locale-source.aarch64        2.34-40.amzn2023.0.2             amazonlinux
gmp.aarch64                        1:6.2.1-2.amzn2023.0.1           amazonlinux
gnupg2-minimal.aarch64             2.3.7-1.amzn2023.0.2             amazonlinux
gzip.aarch64                       1.10-5.amzn2023.0.1              amazonlinux
kernel.aarch64                     6.1.12-17.42.amzn2023            amazonlinux
kernel-tools.aarch64               6.1.12-17.42.amzn2023            amazonlinux
libarchive.aarch64                 3.5.3-2.amzn2023.0.1             amazonlinux
libcurl-minimal.aarch64            7.85.0-1.amzn2023.0.1            amazonlinux
libsepol.aarch64                   3.4-3.amzn2023.0.2               amazonlinux
libsolv.aarch64                    0.7.22-1.amzn2023.0.1            amazonlinux
libxml2.aarch64                    2.9.14-1.amzn2023.0.1            amazonlinux
logrotate.aarch64                  3.20.1-2.amzn2023.0.2            amazonlinux
lua-libs.aarch64                   5.4.4-3.amzn2023.0.1             amazonlinux
lz4-libs.aarch64                   1.9.4-1.amzn2023.0.1             amazonlinux
openssl.aarch64                    1:3.0.5-1.amzn2023.0.3           amazonlinux
openssl-libs.aarch64               1:3.0.5-1.amzn2023.0.3           amazonlinux
pcre2.aarch64                      10.40-1.amzn2023.0.1             amazonlinux
pcre2-syntax.noarch                10.40-1.amzn2023.0.1             amazonlinux
rsync.aarch64                      3.2.6-1.amzn2023.0.2             amazonlinux
vim-common.aarch64                 2:9.0.475-1.amzn2023.0.1         amazonlinux
vim-data.noarch                    2:9.0.475-1.amzn2023.0.1         amazonlinux
vim-enhanced.aarch64               2:9.0.475-1.amzn2023.0.1         amazonlinux
vim-filesystem.noarch              2:9.0.475-1.amzn2023.0.1         amazonlinux
vim-minimal.aarch64                2:9.0.475-1.amzn2023.0.1         amazonlinux
xz.aarch64                         5.2.5-9.amzn2023.0.1             amazonlinux
xz-libs.aarch64                    5.2.5-9.amzn2023.0.1             amazonlinux
zlib.aarch64                       1.2.11-32.amzn2023.0.3           amazonlinux
```

Installa i pacchetti di cui vuoi eseguire l'aggiornamento. Usa `sudo dnf upgrade --releasever=latest` e i nomi dei pacchetti per assicurarti che il pacchetto `system-release` rimanga invariato.

```
$ sudo dnf upgrade --releasever=latest openssl openssl-libs
Last metadata expiration check: 0:01:28 ago on Wed 15 Feb 2023 02:52:21 AM UTC.
Dependencies resolved.
================================================================================
 Package          Arch        Version                      Repository       Size
================================================================================
Upgrading:
 openssl          aarch64     1:3.0.5-1.amzn2023.0.3       amazonlinux     1.1 M
 openssl-libs     aarch64     1:3.0.5-1.amzn2023.0.3       amazonlinux     2.1 M

Transaction Summary
```

```
================================================================================
Upgrade  2 Packages

Total download size: 3.2 M
```

> **Note**
>
> Usando `sudo dnf upgrade --releasever=latest` vengono aggiornati tutti i pacchetti, incluso `system-release`. Quindi, la versione rimane bloccata sul nuovo `system-release` a meno che non imposti l'override persistente.

Uso dell'override persistente con aggiornamento deterministico

Anziché aggiungere `--releasever=latest`, puoi usare l'override persistente per sbloccare il sistema impostando il valore della variabile su *`latest`*.

```
$ echo latest | sudo tee /etc/dnf/vars/releasever
latest
```

```
$ sudo dnf upgrade
Last metadata expiration check: 0:03:36 ago on Wed 15 Feb 2023 02:52:21 AM UTC.
Dependencies resolved.
================================================================================
 Package                 Arch    Version                       Repository   Size
================================================================================
Installing:
 kernel                  aarch64 6.1.73-45.135.amzn2023        amazonlinux  24 M
Upgrading:
 acl                     aarch64 2.3.1-2.amzn2023.0.1          amazonlinux  72 k
 alternatives            aarch64 1.15-2.amzn2023.0.1           amazonlinux  36 k
 amazon-ec2-net-utils    noarch  2.3.0-1.amzn2023.0.1          amazonlinux  16 k
 at                      aarch64 3.1.23-6.amzn2023.0.1         amazonlinux  60 k
 attr                    aarch64 2.5.1-3.amzn2023.0.1          amazonlinux  59 k
 audit                   aarch64 3.0.6-1.amzn2023.0.1          amazonlinux 249 k
 audit-libs              aarch64 3.0.6-1.amzn2023.0.1          amazonlinux 116 k
 aws-c-auth-libs         aarch64 0.6.5-6.amzn2023.0.2          amazonlinux  79 k
 aws-c-cal-libs          aarch64 0.5.12-7.amzn2023.0.2         amazonlinux  34 k
 aws-c-common-libs       aarch64 0.6.14-6.amzn2023.0.2         amazonlinux 119 k
 aws-c-compression-libs  aarch64 0.2.14-5.amzn2023.0.2         amazonlinux  22 k
 aws-c-event-stream-libs aarch64 0.2.7-5.amzn2023.0.2          amazonlinux  47 k
```

```
 aws-c-http-libs          aarch64 0.6.8-6.amzn2023.0.2         amazonlinux 147 k
 aws-c-io-libs            aarch64 0.10.12-5.amzn2023.0.6       amazonlinux 109 k
 aws-c-mqtt-libs          aarch64 0.7.8-7.amzn2023.0.2         amazonlinux  61 k
 aws-c-s3-libs            aarch64 0.1.27-5.amzn2023.0.3        amazonlinux  54 k
 aws-c-sdkutils-libs      aarch64 0.1.1-5.amzn2023.0.2         amazonlinux  26 k
 aws-checksums-libs       aarch64 0.1.12-5.amzn2023.0.2        amazonlinux  50 k
 awscli-2                 noarch  2.7.8-1.amzn2023.0.4         amazonlinux 7.3 M
 basesystem               noarch  11-11.amzn2023.0.1           amazonlinux 7.8 k
 bash                     aarch64 5.1.8-2.amzn2023.0.1         amazonlinux 1.6 M
 bash-completion          noarch  1:2.11-2.amzn2023.0.1        amazonlinux 292 k
 bc                       aarch64 1.07.1-14.amzn2023.0.1       amazonlinux 120 k
 bind-libs                aarch64 32:9.16.27-1.amzn2023.0.1    amazonlinux 1.2 M
 bind-license             noarch  32:9.16.27-1.amzn2023.0.1    amazonlinux  14 k
 bind-utils               aarch64 32:9.16.27-1.amzn2023.0.1    amazonlinux 206 k
 binutils                 aarch64 2.38-20.amzn2023.0.3         amazonlinux 4.6 M
 boost-filesystem         aarch64 1.75.0-4.amzn2023.0.1        amazonlinux  55 k
 boost-system             aarch64 1.75.0-4.amzn2023.0.1        amazonlinux  14 k
 boost-thread             aarch64 1.75.0-4.amzn2023.0.1        amazonlinux  54 k
 bzip2                    aarch64 1.0.8-6.amzn2023.0.1         amazonlinux  53 k
 bzip2-libs               aarch64 1.0.8-6.amzn2023.0.1         amazonlinux  44 k
 c-ares                   aarch64 1.17.2-1.amzn2023.0.1        amazonlinux 107 k
 ca-certificates          noarch  2021.2.50-1.0.amzn2023.0.3   amazonlinux 343 k
 checkpolicy              aarch64 3.4-3.amzn2023.0.1           amazonlinux 345 k
 chkconfig                aarch64 1.15-2.amzn2023.0.1          amazonlinux 162 k
 chrony                   aarch64 4.2-7.amzn2023.0.4           amazonlinux 314 k
 cloud-init               noarch  22.2.2-1.amzn2023.1.7        amazonlinux 1.1 M
 cloud-utils-growpart     aarch64 0.31-8.amzn2023.0.2          amazonlinux  31 k
 coreutils                aarch64 8.32-30.amzn2023.0.2         amazonlinux 1.1 M
 coreutils-common         aarch64 8.32-30.amzn2023.0.2         amazonlinux 2.0 M
 cpio                     aarch64 2.13-10.amzn2023.0.1         amazonlinux 269 k
 cracklib                 aarch64 2.9.6-27.amzn2023.0.1        amazonlinux  83 k
 cracklib-dicts           aarch64 2.9.6-27.amzn2023.0.1        amazonlinux 3.6 M
 crontabs                 noarch  1.11-24.20190603git.amzn2023.0.1
                                                               amazonlinux  19 k
 crypto-policies          noarch  20230128-1.gitdfb10ea.amzn2023.0.1
                                                               amazonlinux  61 k
 crypto-policies-scripts noarch  20230128-1.gitdfb10ea.amzn2023.0.1
                                                               amazonlinux  81 k
...
Installing dependencies:
 amazon-linux-repo-cdn    noarch  2023.0.20230210-0.amzn2023   amazonlinux  16 k
 xxhash-libs              aarch64 0.8.0-3.amzn2023.0.1         amazonlinux  32 k
Installing weak dependencies:
 amazon-chrony-config     noarch  4.2-7.amzn2023.0.4           amazonlinux  14 k
```

```
 gawk-all-langpacks      aarch64 5.1.0-3.amzn2023.0.1         amazonlinux 207 k

Transaction Summary
================================================================================
Install    5 Packages
Upgrade  413 Packages

Total download size: 199 M
```

> **Note**
>
> Se hai usato la variabile di override `/etc/dnf/vars/releasever`, utilizza il comando seguente per ripristinare il comportamento di blocco predefinito cancellando il valore di override.
>
> ```
> $ sudo rm /etc/dnf/vars/releasever
> ```

Applicazione di patch Kernel Live su AL2023

È possibile utilizzare Kernel Live Patching per AL2023 per applicare vulnerabilità di sicurezza e patch di bug critici a un kernel Linux in esecuzione senza riavviare o interrompere le applicazioni in esecuzione. Inoltre, Kernel Live Patching può aiutarti a migliorare la disponibilità delle applicazioni mantenendo al contempo l'infrastruttura aggiornata e protetta.

AWS rilascia due tipi di patch live del kernel per AL2023:

- 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: include correzioni per bug critici e problemi di stabilità che non sono associati ai CVE.

AWS fornisce patch live del kernel per una versione del kernel AL2023 per un massimo di 3 mesi dopo il suo rilascio. Dopo tale periodo, è necessario eseguire l'aggiornamento a una versione del kernel successiva per continuare a ricevere patch live del kernel.

Le patch live del kernel AL2023 sono rese disponibili come pacchetti RPM firmati nei repository AL2023 esistenti. Le patch possono essere installate su singole istanze utilizzando i flussi di lavoro del gestore di pacchetti DNF esistenti. In alternativa, possono essere installati su un gruppo di istanze gestite utilizzando AWS Systems Manager.

Kernel Live Patching su AL2023 è fornito senza costi aggiuntivi.

Argomenti

Limitazioni

Durante l'applicazione di una patch live del kernel, non è possibile eseguire l'ibernazione, utilizzare strumenti di debug avanzati (come `SystemTap`, `kprobes` e strumenti basati su `eBPF`) né accedere ai file di output `ftrace` utilizzati dall'infrastruttura Kernel Live Patching.

Configurazioni e prerequisiti supportati

Kernel Live Patching è supportata su istanze Amazon EC2 e macchine virtuali on-premise che eseguono AL2023.

Per usare Kernel Live Patching su AL2023, è necessario utilizzare:

- Un'architettura `x86_64` o `ARM64` a 64 bit
- Kernel versione `6.1`

Requisiti per le policy

Per scaricare pacchetti dai repository AL2023, Amazon EC2 deve accedere ai bucket Amazon S3 di proprietà del servizio. Se utilizzi un endpoint Amazon Virtual Private Cloud (VPC) per Amazon S3 nel tuo ambiente, assicurati che la policy degli endpoint VPC consenta l'accesso a tali bucket pubblici.

La tabella seguente descrive il bucket Amazon S3 a cui Amazon EC2 potrebbe dover accedere per Kernel Live Patching.

ARN di bucket S3	Descrizione
*arn:aws:s3: ::al2023-repos-region -de612dc2/**	Bucket Amazon S3 contenente repository AL2023

Utilizzo di Kernel Live Patching

È possibile abilitare e utilizzare Kernel Live Patching su singole istanze utilizzando la riga di comando sull'istanza stessa. In alternativa, è possibile abilitare e utilizzare Kernel Live Patching su un gruppo di istanze gestite utilizzando AWS Systems Manager.

Le sezioni seguenti spiegano come abilitare e utilizzare Kernel Live Patching su singole istanze utilizzando la riga di comando.

Per ulteriori informazioni sull'abilitazione e l'utilizzo di Kernel Live Patching su un gruppo di istanze gestite, consulta Utilizzo di Kernel Live Patching sulle istanze AL2023 nella Guida per l'utente di AWS Systems Manager .

Argomenti

- Abilitazione di Kernel Live Patching
- Visualizzazione delle patch live del kernel disponibili
- Applicazione delle patch live del kernel
- Visualizzazione delle patch live del kernel applicate
- Disabilitazione di Kernel Live Patching

Abilitazione di Kernel Live Patching

Kernel Live Patching è disabilitata per impostazione predefinita su AL2023. Per utilizzare l'applicazione di patch live, è necessario installare il plugin DNF per Kernel Live Patching e abilitare la funzionalità di applicazione di patch live.

Per abilitare Kernel Live Patching

1. Le patch live del kernel sono disponibili per AL2023 con versione del kernel `6.1` o successive. Per controllare la versione del kernel, eseguire il seguente comando.

   ```
   $ sudo dnf list kernel
   ```

2. Installare il plugin DNF per Kernel Live Patching.

   ```
   $ sudo dnf install -y kpatch-dnf
   ```

3. Abilitare il plugin DNF per Kernel Live Patching.

   ```
   $ sudo dnf kernel-livepatch -y auto
   ```

   Questo comando installa anche l'ultima versione dell'RPM della patch live del kernel dai repository configurati.

4. Per confermare che il plugin DNF per Kernel Live Patching è stato installato correttamente, eseguire il seguente comando.

   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.

   ```
   $ sudo rpm -qa | grep kernel-livepatch
   dnf-plugin-kernel-livepatch-1.0-0.11.amzn2023.noarch
   kernel-livepatch-6.1.12-17.42-1.0-0.amzn2023.x86_64
   ```

5. Installare il pacchetto kpatch.

   ```
   $ sudo dnf install -y kpatch-runtime
   ```

6. Aggiornare il servizio kpatch se è stato precedentemente installato.

   ```
   $ sudo dnf update kpatch-runtime
   ```

7. 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
```

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 di sicurezza di AL2023, inclusi gli avvisi per patch live del kernel, consulta la pagina 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 inoltre individuare le patch in tempo reale del kernel disponibili per gli advisory e i CVE utilizzando la riga di comando.

Per elencare tutte le patch live del kernel disponibili per le consulenze

Utilizza il seguente comando.

```
$ sudo dnf updateinfo list
Last metadata expiration check: 1:06:23 ago on Mon 13 Feb 2023 09:28:19 PM UTC.
ALAS2LIVEPATCH-2021-123   important/Sec. kernel-
livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
ALAS2LIVEPATCH-2022-124   important/Sec. kernel-
livepatch-6.1.12-17.42-1.0-3.amzn2023.x86_64
```

Per elencare tutte le patch live del kernel disponibili per i CVE

Utilizza il seguente comando.

```
$ sudo dnf updateinfo list cves
Last metadata expiration check: 1:07:26 ago on Mon 13 Feb 2023 09:28:19 PM UTC.
CVE-2022-0123    important/Sec. kernel-livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
CVE-2022-3210    important/Sec. kernel-livepatch-6.1.12-17.42-1.0-3.amzn2023.x86_64
```

Applicazione delle patch live del kernel

Le patch live del kernel vengono applicate utilizzando il gestore di pacchetti DNF nello stesso modo in cui si applicano aggiornamenti regolari. Il plugin DNF per Kernel Live Patching gestisce le patch live del kernel da applicare ed elimina la necessità di riavviare.

> **Tip**
>
> Si consiglia di aggiornare regolarmente il kernel utilizzando Kernel Live Patching per assicurarsi che rimanga sicuro e aggiornato.

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. Applicare la patch live del kernel per il kernel AL2023.

   ```
   $ sudo dnf install kernel-livepatch-kernel_version-package_version.amzn2023.x86_64
   ```

   Ad esempio, il seguente comando applica una patch live del kernel per la versione kernel `6.1.12-17.42` di AL2023.

   ```
   $ sudo dnf install kernel-livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
   ```

Per applicare eventuali patch live del kernel disponibili insieme ai normali aggiornamenti di sicurezza

Utilizzare il seguente comando.

```
$ sudo dnf 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 kernel AL2023 riceve patch live del kernel per un periodo di 3 mesi. Dopo questo periodo, non vengono rilasciate nuove patch live del kernel per tale versione del kernel.

- Per continuare a ricevere patch live del kernel dopo 3 mesi, è necessario riavviare l'istanza per passare alla nuova versione del kernel. L'istanza continua a ricevere le patch live del kernel per i successivi 3 mesi dopo l'aggiornamento.
- Per controllare la finestra di supporto per la versione del kernel, esegui il seguente comando:

```
$ sudo dnf kernel-livepatch support
```

Visualizzazione delle patch live del kernel applicate

Per visualizzare le patch live del kernel applicate

Utilizzare il seguente comando.

```
$ sudo kpatch list
Loaded patch modules:
livepatch_CVE_2022_36946 [enabled]

Installed patch modules:
livepatch_CVE_2022_36946 (6.1.57-29.131.amzn2023.x86_64)
livepatch_CVE_2022_36946 (6.1.57-30.131.amzn2023.x86_64)
```

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.

> **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.

- Disabilita l'uso di livepatches:
  1. Disabilita il plugin:

```
$ sudo dnf kernel-livepatch manual
```

2. Disabilita il servizio kpatch:

```
$ sudo systemctl disable --now kpatch.service
```

- Rimuovi completamente gli strumenti livepatch:

1. Rimuovi il plugin:

```
$ sudo dnf remove kpatch-dnf
```

2. Rimuovi kpatch-runtime:

```
$ sudo dnf remove kpatch-runtime
```

3. Rimuovi tutte le livepatches installate:

```
$ sudo dnf remove kernel-livepatch\*
```

Guida introduttiva alla programmazione dei runtime su AL2023

AL2023 fornisce diverse versioni di alcuni runtime linguistici. Lavoriamo con progetti upstream che supportano più versioni contemporaneamente. Scopri come installare e gestire questi pacchetti dotati di versioni con nomi utilizzando il comando `dnf` per cercare e installare questi pacchetti.

I seguenti argomenti descrivono l'esistenza di ciascun ecosistema linguistico in AL2023.

Argomenti

C, C++ e Fortran in AL2023

AL2023 include sia la GNU Compiler Collection (GCC) che il Clang frontend per LLVM (Low Level Virtual Machine).

La versione principale di AL2023 GCC rimarrà costante per tutta la durata di AL2023. Le versioni secondarie introducono correzioni di bug e potrebbero essere incluse nei rilasci AL2023. Per altre correzioni di bug, prestazioni e sicurezza potrebbe essere eseguito il backporting alla versione principale di GCC fornita in AL2023.

AL2023 include la versione 11 di GCC con i frontend C (`gcc`), C++ () e Fortran (`g++`). `gfortran`

AL2023 non abilita i frontend (), Ada (`gnat`), Objective-C o Go `gcc-go` Objective-C++.

I flag predefiniti del compilatore con cui sono creati gli RPM AL2023 includono flag di ottimizzazione e rafforzamento. Per creare il tuo codice con GCC, ti consigliamo di includere flag di ottimizzazione e rafforzamento.

> **Note**
>
> Quando `gcc --version` viene richiamato, viene visualizzata una stringa di versione come `gcc (GCC) 11.3.1 20221121 (Red Hat 11.3.1-4)`. `Red Hat` si riferisce al ramo del fornitore GCC su cui si basa il pacchetto di Amazon Linux GCC. In base all'URL di segnalazione dei bug mostrato da`gcc --help`, tutte le segnalazioni di bug e le richieste di supporto devono essere indirizzate ad Amazon Linux.
> Per maggiori informazioni su alcune delle modifiche a lungo termine in questo ramo del fornitore, come la `__GNUC_RH_RELEASE__` macro, vedi i sorgenti dei pacchetti Fedora.

Per ulteriori informazioni sulla toolchain di base, vedere. Pacchetti di toolchain principali glibc, gcc, binutils

Per ulteriori informazioni su AL2023 e sulla sua relazione con altre distribuzioni Linux, vedere. Relazione con Fedora

Per ulteriori informazioni sulla modifica della tripletta del compilatore in AL2023 rispetto a AL2, vedere. Tripletta del compilatore

Go in AL2023

Potresti voler creare il tuo codice scritto Gosu Amazon Linux e utilizzare una toolchain fornita con AL2023. Analogamente a AL2, AL2023 aggiornerà la Go toolchain per tutta la durata del sistema operativo. Questo potrebbe avvenire in risposta a qualsiasi CVE nella toolchain che forniamo o come parte di un rilascio trimestrale.

Goè una lingua 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 AL2023 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 in AL2023 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 AL2023, le versioni precedenti dei pacchetti non vengono rimosse dai repository. Se è necessaria una Go toolchain precedente, puoi 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 AL2023, puoi utilizzare la Go toolchain inclusa in AL2023 con la consapevolezza che questa toolchain potrebbe continuare per tutta la durata di AL2023.

Funzioni Lambda AL2023 scritte in Go

Durante la Go compilazione in codice nativo, Lambda Go tratta come un runtime personalizzato. Puoi usare il `provided.al2023` runtime per distribuire Go funzioni su AL2023 su Lambda.

Per ulteriori informazioni, consulta Creazione di funzioni Lambda Go nella Guida per gli AWS Lambda sviluppatori.

Java in AL2023

AL2023 fornisce diverse versioni di Amazon Corretto per supportare carichi di lavoro Java basati. Tutti i pacchetti Java basati inclusi in AL2023 sono costruiti con. Amazon Corretto 17 17

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.

È disponibile un pacchetto Amazon Corretto per ciascuno dei pacchetti Corretto 1.8.0, Corretto 11 e Corretto 17.

Ogni versione di Corretto in AL2023 è supportata per lo stesso periodo della versione Corretto o fino alla fine del ciclo di vita di AL2023, a seconda di quale delle due situazioni si verifichi per prima. Per ulteriori informazioni, consulta le dichiarazioni di supporto dei pacchetti Amazon Linux e le domande frequenti su Amazon Corretto.

Perl in AL2023

AL2023 fornisce la versione 5.32 del Perllinguaggio di programmazione.

Sebbene Perl abbia fornito un alto grado di compatibilità linguistica come parte di Perl 5 versioni negli ultimi decenni, non si prevede che Amazon Linux passi dalla versione Perl 5.32 durante la versione AL2023. Amazon Linux continuerà ad applicare le patch di sicurezza Perl per tutta la durata di AL2023 in conformità con le nostre dichiarazioni di supporto ai pacchetti.

Moduli Perl in AL2023

Vari Perl moduli sono impacchettati come RPM in AL2023. Sebbene siano disponibili molti Perl moduli come RPM, Amazon Linux non mira a impacchettare tutti i Perl moduli possibili. I moduli impacchettati come RPM potrebbero essere utilizzati da altri pacchetti RPM del sistema operativo, quindi Amazon Linux darà la priorità a tali patch di sicurezza rispetto ai puri aggiornamenti delle funzionalità.

AL2023 include anche la possibilità per Perl gli sviluppatori di utilizzare il `CPAN` gestore di pacchetti idiomatico per i moduli. Perl

PHP in AL2023

AL2023 attualmente fornisce due versioni del linguaggio di PHPprogrammazione, ciascuna supportata per lo stesso periodo di tempo dell'PHPupstream. Per ulteriori informazioni, vedere Package support statements.

Con AL2023, è possibile utilizzare le nuove funzionalità della versione PHP 8.2, continuando a supportare le applicazioni che richiedono PHP la versione 8.1.

Migrazione da versioni PHP precedenti

La PHP comunità upstream ha messo insieme una documentazione completa sulla migrazione per passare alla versione PHP 8.2 dalla 8.1. PHP Esiste anche la documentazione per la migrazione da PHP 8.0 a 8.1.

AL2 include PHP 8.0, 8.1 e 8.2 per `amazon-linux-extras` consentire un facile percorso di aggiornamento ad AL2023.

Migrazione da PHP versioni 7.x

> **Note**
>
> Il PHPprogetto mantiene un elenco e una pianificazione delle versioni supportate, nonché un elenco di filiali non supportate.
> Quando AL2023 è stato rilasciato, tutte le versioni 7.x e 5.x di AL2023 non PHPerano supportate dalla PHP community e non erano incluse come opzioni in AL2023.

La PHP comunità upstream ha messo insieme una documentazione completa sulla migrazione per passare alla versione 8.0 dalla 7.4. PHP PHP In combinazione con la documentazione a cui si fa riferimento nella sezione precedente sulla migrazione alla versione PHP 8.1 e PHP 8.2, è possibile migrare l'applicazione basata su una versione moderna. PHP PHP

> **Note**
>
> AL2 include PHP 7,1, 7,2, 7,3 e 7,4 pollici. `amazon-linux-extras` È importante notare che tutti questi Extra sono end-of-life e non sono garantiti ulteriori aggiornamenti di sicurezza.

Moduli PHP in AL2023

AL2023 include molti PHP moduli inclusi in PHP Core. AL2023 non mira a includere tutti i pacchetti nella PHPExtension Community Library (PECL).

Python in AL2023

AL2023 ha rimosso la Python versione 2.7 e tutti i componenti necessari Python sono ora scritti per funzionare con Python 3.

AL2023 rende disponibile Python 3 `/usr/bin/python3` per mantenere la compatibilità con il codice del cliente, oltre al codice Python fornito con AL2023, che Python rimarrà 3.9 per tutta la vita di AL2023.

La versione di python a cui `/usr/bin/python3` punta è considerata il sistema Python e per AL2023 questa è la 3.9. Python

Le versioni più recenti diPython, come la Python 3.11, sono rese disponibili come pacchetti in AL2023 e sono supportate per tutta la durata delle versioni upstream. Per informazioni su quanto tempo è supportato Python 3.11, vedere Python 3.11.

È possibile installare contemporaneamente più versioni di Python su AL2023. Sebbene `/usr/bin/python3` sarà sempre Python 3.9, ogni versione di Python ha uno spazio dei nomi e può essere trovata in base al numero di versione. Ad esempio, se è installato `python3.11`, `/usr/bin/python3.11` esisterà insieme a `/usr/bin/python3.9` e al symlink `/usr/bin/python3` a `/usr/bin/python3.9`.

> **Note**
>
> Non modificate il punto a cui punta il `/usr/bin/python3` collegamento simbolico perché ciò potrebbe compromettere la funzionalità di base di AL2023.

Moduli Python in AL2023

Vari Python moduli sono impacchettati come RPM in AL2023. In genere, gli RPM per i moduli Python vengono sviluppati solo per la versione di sistema di Python.

Rust in AL2023

Potresti voler creare il loro codice scritto Rustsu Amazon Linux e potresti voler utilizzare una toolchain fornita con AL2023.

Analogamente a AL2, AL2023 aggiornerà la Rust toolchain per tutta la durata del sistema operativo. Questo potrebbe avvenire in risposta a qualsiasi CVE nella toolchain che forniamo o come parte di un rilascio trimestrale.

Rust è un linguaggio che cambia in modo relativamente veloce, con nuovi rilasci all'incirca ogni sei settimane. I rilasci potrebbero aggiungere nuove funzionalità di linguaggio o di libreria standard. Sebbene AL2023 incorporerà nuove versioni della Rust toolchain nel corso del suo ciclo di vita, ciò non sarà in linea con le versioni upstream. Rust Pertanto, l'utilizzo della Rust toolchain fornita in AL2023 potrebbe non essere adatto se si desidera creare Rust codice utilizzando funzionalità all'avanguardia del linguaggio. Rust

Nel corso del ciclo di vita di AL2023, le versioni dei vecchi pacchetti non vengono rimosse dai repository. Se è necessaria una Rust toolchain precedente, puoi scegliere di rinunciare alle correzioni di bug e sicurezza delle Rust toolchain più recenti e installare una versione precedente dai repository utilizzando gli stessi meccanismi disponibili per qualsiasi RPM.

Se desideri creare il tuo Rust codice su AL2023, puoi utilizzare la Rust toolchain inclusa in AL2023 con la consapevolezza che questa toolchain potrebbe continuare per tutta la durata di AL2023.

Funzioni Lambda AL2023 scritte in Rust

Poiché viene Rust compilato in codice nativo, Lambda Rust tratta come un runtime personalizzato. Puoi usare il `provided.al2023` runtime per distribuire Rust funzioni su AL2023 su Lambda.

Per ulteriori informazioni, consulta Creazione di funzioni Lambda Rust nella Guida per gli AWS Lambda sviluppatori.

Sicurezza e conformità in Amazon Linux 2023

> **Important**
>
> Se desideri segnalare una vulnerabilità o hai un problema di sicurezza relativo ai servizi AWS cloud o ai progetti open source, contatta la AWS sicurezza tramite la nostra pagina di segnalazione delle vulnerabilità o direttamente con un'e-mail a aws-security@amazon.com. Se desideri proteggere il contenuto del tuo invio, puoi utilizzare la nostra chiave PGP.

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 aspetto 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. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano a AL2023, consulta AWS Servizi nell'ambito del programma di conformitàAWS Servizi nell'ambito del programma .
- 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.

Argomenti

Avvisi di sicurezza di Amazon Linux per AL2023

Anche se ci impegniamo a fondo per rendere sicuro Amazon Linux, talvolta si verificheranno problemi di sicurezza che devono essere risolti. Quando è disponibile una correzione, viene emesso un avviso. La sede principale in cui pubblichiamo gli avvisi è Amazon Linux Security Center (ALAS). Per ulteriori informazioni, consulta la pagina Amazon Linux Security Center.

> **Important**
>
> Se desideri segnalare una vulnerabilità o hai un problema di sicurezza relativo ai servizi AWS cloud o ai progetti open source, contatta la AWS sicurezza tramite la nostra pagina di segnalazione delle vulnerabilità o direttamente inviando un'e-mail a aws-security@amazon.com. Se desideri proteggere il contenuto del tuo invio, puoi utilizzare la nostra chiave PGP.

Le informazioni sui problemi e gli aggiornamenti pertinenti che riguardano AL2023 sono pubblicate dal team di Amazon Linux in diverse località. È comune che gli strumenti di sicurezza recuperino informazioni da queste fonti principali e ti presentino i risultati. Pertanto, potresti non interagire direttamente con le fonti primarie pubblicate da Amazon Linux, ma con l'interfaccia fornita dai tuoi strumenti preferiti, come Amazon Inspector.

Annunci sull'Amazon Linux Security Center

Gli annunci di Amazon Linux vengono forniti per articoli che non rientrano in un avviso. Questa sezione contiene annunci riguardanti ALAS stesso, oltre a informazioni che non rientrano in un avviso. Per ulteriori informazioni, consulta gli annunci di Amazon Linux Security Center (ALAS).

Ad esempio, l'annuncio 2021-001 - Amazon Linux Hotpatch per Apache Log4j rientra in un annuncio piuttosto che in un avviso. In questo annuncio, Amazon Linux ha aggiunto un pacchetto per aiutare i clienti a mitigare un problema di sicurezza in software che non faceva parte di Amazon Linux.

L'Amazon Linux Security Center CVE Explorer è stato annunciato anche negli annunci ALAS. Per ulteriori informazioni, consulta Nuovo sito Web per CVes.

Domande frequenti su Amazon Linux Security Center

Per le risposte ad alcune domande frequenti su ALAS e su come Amazon Linux valuta i CVE, consulta le domande frequenti (FAQ) di Amazon Linux Security Center (ALAS).

Impostazione delle modalità SELinux per AL2023

Per impostazione predefinita, Security Enhanced Linux (SELinux) è `enabled` impostata sulla `permissive` modalità AL2023. In modalità di autorizzazione, le negazioni di autorizzazione vengono registrate ma non applicate. SELinux è una raccolta di funzionalità e utilità del kernel in grado di fornire un'architettura per il controllo degli accessi obbligatorio (MAC) robusta e flessibile per i principali sottosistemi del kernel.

SELinux fornisce un meccanismo avanzato per applicare la separazione delle informazioni in base a requisiti di riservatezza e integrità. Questa separazione delle informazioni riduce le minacce di manomissione e aggiramento dei meccanismi di sicurezza delle applicazioni. Inoltre limita i danni che possono essere causati da applicazioni dannose o difettose.

SELinux include una serie di esempi di file di configurazione delle policy di sicurezza progettati per soddisfare gli obiettivi di sicurezza quotidiani.

Per ulteriori informazioni sulle caratteristiche e funzionalità di SELinux, consulta le pagine dedicate a SELinux Notebook e linguaggi delle policy.

Argomenti

Stato e modalità SELinux predefiniti per AL2023

Per AL2023, SELinux di default è `enabled` impostato su mode. `permissive` In modalità `permissive`, le negazioni di autorizzazione vengono registrate ma non applicate.

I comandi **`getenforce`** o **`sestatus`** indicano lo stato, la policy e la modalità attuali di SELinux.

Con lo stato predefinito impostato su `enabled` e `permissive`, il comando **`getenforce`** restituisce `permissive`.

Il **`sestatus`** comando restituisce lo stato di SELinux e la politica corrente di SELinux, come mostrato nell'esempio seguente:

```
$ sestatus
SELinux status:                 enabled
```

```
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

Quando si esegue SELinux in `permissive` modalità, gli utenti potrebbero etichettare i file in modo errato. Quando esegui SELinux nello stato `disabled`, i file non vengono etichettati. Sia i file errati che quelli senza etichetta possono causare problemi quando passi alla modalità `enforcing`.

SELinux rietichetta automaticamente i file per evitare questo problema. SELinux previene i problemi di etichettatura con la rietichettatura automatica quando si modifica lo stato in `enabled`.

Passaggio alla modalità **`enforcing`**

Quando si esegue SELinux in `enforcing` modalità, l'SELinuxutilità è `enforcing` la politica configurata. SELinuxgoverna le funzionalità di determinate applicazioni consentendo o negando l'accesso in base alle regole della policy.

Per trovare la SELinux modalità corrente, esegui il `getenforce` comando.

```
getenforce
Permissive
```

Modifica del file di configurazione per abilitare la modalità **`enforcing`**

Per cambiare la modalità in`enforcing`, utilizzare la procedura seguente.

1. Modifica il file `/etc/selinux/config` per passare alla modalità `enforcing`. L'`SELINUX`impostazione dovrebbe essere simile all'esempio seguente.

   ```
   SELINUX=enforcing
   ```

2. Riavvia il sistema per completare il passaggio alla modalità `enforcing`.

   ```
   $ sudo reboot
   ```

All'avvio successivo, SELinux ridefinisce tutti i file e le directory del sistema. SELinuxaggiunge anche il SELinux contesto per i file e le directory che sono stati creati quando era. SELinux `disabled`

Dopo il passaggio alla `enforcing` modalità, SELinux potrebbe negare alcune azioni a causa di regole di SELinux policy errate o mancanti. È possibile visualizzare le azioni SELinux negate con il seguente comando.

```
$ sudo ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts recent
```

Uso di cloud-init per abilitare la modalità **`enforcing`**

In alternativa, quando avvii l'istanza, passa la seguente `cloud-config` come dati utente per abilitare la modalità `enforcing`.

```
#cloud-config
selinux:
  mode: enforcing
```

Per impostazione predefinita, questa impostazione causa il riavvio dell'istanza. Per una maggiore stabilità, consigliamo di riavviare l'istanza. Tuttavia, se preferisci, puoi saltare il riavvio fornendo la seguente `cloud-config`.

```
#cloud-config
selinux:
  mode: enforcing
  selinux_no_reboot: 1
```

Opzione per disabilitare SELinux per AL2023

Quando si disattivaSELinux, la SELinux policy non viene caricata o applicata e i messaggi di Access Vector Cache (AVC) non vengono registrati. Perdi tutti i vantaggi della corsa. SELinux

Invece di disabilitareSELinux, consigliamo di utilizzare la `permissive` modalità. L'esecuzione in `permissive` modalità costa solo un po' di più rispetto alla disattivazione SELinux completa. La transizione da una `permissive` `enforcing` modalità all'altra richiede una regolazione della configurazione molto inferiore rispetto al ritorno alla `enforcing` modalità dopo la disattivazione. SELinux Puoi etichettare i file, e il sistema può tracciare e registrare i log delle azioni che la policy attiva potrebbe aver negato.

Passare alla modalità SELinux`permissive`

Quando si esegue SELinux in `permissive` modalità, la SELinux politica non viene applicata. In `permissive` modalità, SELinux registra i messaggi AVC ma non nega le operazioni. È possibile utilizzare questi messaggi AVC per la risoluzione dei problemi, il debug e il miglioramento delle politiche. SELinux

Per passare SELinux alla modalità permissiva, utilizzare i seguenti passaggi.

1. Modifica il file `/etc/selinux/config` per passare alla modalità `permissive`. Il `SELINUX` valore dovrebbe essere simile all'esempio seguente.

```
SELINUX=permissive
```

2. Riavvia il sistema per completare il passaggio alla modalità `permissive`.

```
sudo reboot
```

Disabilitazione di SELinux

Quando si disattivaSELinux, la SELinux policy non viene caricata o applicata e i messaggi AVC non vengono registrati. Perdi tutti i vantaggi della corsa. SELinux

Per disabilitareSELinux, utilizzare i seguenti passaggi.

1. Assicurati che il `grubby` pacchetto sia installato.

```
rpm -q grubby
grubby-version
```

2. Configura il bootloader per aggiungere `selinux=0` alla riga di comando del kernel.

```
sudo grubby --update-kernel ALL --args selinux=0
```

3. Riavvia il sistema.

```
sudo reboot
```

4. Esegui il `getenforce` comando per confermare che SELinux sia così`Disabled`.

```
$ getenforce
Disabled
```

Per ulteriori informazioni suSELinux, consulta SELinuxNotebook e SELinuxconfigurazione.

Abilita la modalità FIPS su AL2023

Questa sezione spiega come abilitare gli standard FIPS (Federal Information Processing Standard) su AL2023. Per ulteriori informazioni sul FIPS, consulta:

- Federal Information Processing Standard (FIPS)
- Domande frequenti sulla conformità: Federal Information Processing Standard

> **Note**
>
> Questa sezione spiega come abilitare la modalità FIPS in AL2023, ma non parla dello stato di certificazione dei moduli crittografici AL2023.

Prerequisiti

- Un'istanza Amazon EC2 di AL2023 (AL2023.2 o versioni successive) esistente con accesso a Internet per scaricare i pacchetti richiesti. Per ulteriori informazioni sull'avvio di un'istanza Amazon EC2 di AL2023, consulta Avvio di AL2023 utilizzando la console Amazon EC2.
- Devi eseguire la connessione all'istanza Amazon EC2 utilizzando SSH o AWS Systems Manager. Per ulteriori informazioni, consulta Connessione alle istanze AL2023.

> **Important**
>
> Le chiavi utente SSH ED25519 non sono supportate in modalità FIPS. Se hai avviato l'istanza Amazon EC2 utilizzando una coppia di chiavi SSH ED25519, devi generare nuove chiavi utilizzando un altro algoritmo (come RSA); altrimenti, potresti perdere l'accesso all'istanza dopo aver abilitato la modalità FIPS. Per ulteriori informazioni, consulta la pagina che spiega come creare le coppie di chiavi nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Abilitazione della modalità FIPS

1. Connettiti all'istanza AL2023 utilizzando SSH o AWS Systems Manager.
2. Verifica che il sistema sia aggiornato. Per ulteriori informazioni, consulta Gestione degli aggiornamenti dei pacchetti e del sistema operativo in AL2023.
3. Assicurati che le `crypto-policies` utilità siano installate e. up-to-date

   ```
   sudo dnf -y install crypto-policies crypto-policies-scripts
   ```

4. Abilita la modalità FIPS eseguendo il seguente comando.

   ```
   sudo fips-mode-setup --enable
   ```

5. Riavvia l'istanza utilizzando il comando seguente.

   ```
   sudo reboot
   ```

6. Per verificare che la modalità FIPS sia abilitata, riconnettiti all'istanza ed esegui il comando seguente.

   ```
   sudo fips-mode-setup --check
   ```

   Il seguente esempio di output mostra che la modalità FIPS è abilitata:

   ```
   FIPS mode is enabled.
   Initramfs fips module is enabled.
   The current crypto policy (FIPS) is based on the FIPS policy.
   ```

Indurimento del kernel AL2023

Il kernel Linux 6.1 in AL2023 è configurato e costruito con diverse opzioni e funzionalità di rafforzamento.

Opzioni di rafforzamento del kernel (indipendenti dall'architettura)

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_ACPI_CUSTOM_METHOD	n	n
CONFIG_BINFMT_MISC	m	m
CONFIG_BUG	y	y
CONFIG_BUG_ON_DATA_CORRUPTION	y	y
CONFIG_CFI_CLANG	N/D	N/D
CONFIG_CFI_PERMISSIVE	N/D	N/D
CONFIG_COMPAT	y	y
CONFIG_COMPAT_BRK	n	n
CONFIG_COMPAT_VDSO	N/D	n
CONFIG_DEBUG_CREDENTIALS	n	n
CONFIG_DEBUG_LIST	y	y
CONFIG_DEBUG_NOTIFIERS	n	n
CONFIG_DEBUG_SG	n	n
CONFIG_DEBUG_VIRTUAL	n	n
CONFIG_DEBUG_WX	n	n
CONFIG_DEFAULT_MMAP_MIN_ADDR	65536	65536
CONFIG_DEVKMEM	N/D	N/D

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_DEVMEM	n	n
CONFIG_EFI_DISABLE_PCI_DMA	n	n
CONFIG_FORTIFY_SOURCE	y	y
CONFIG_HARDENED_USERCOPY	y	y
CONFIG_HARDENED_USERCOPY_FALLBACK	N/D	N/D
CONFIG_HARDENED_USERCOPY_PAGESPAN	N/D	N/D
CONFIG_HIBERNATION	y	y
CONFIG_HW_RANDOM_TPM	N/D	N/D
CONFIG_INET_DIAG	m	m
CONFIG_INIT_ON_ALLOC_DEFAULT_ON	n	n
CONFIG_INIT_ON_FREE_DEFAULT_ON	n	n
CONFIG_INIT_STACK_ALL_ZERO	N/D	N/D
CONFIG_IOMMU_DEFAULT_DMA_STRICT	n	n
CONFIG_IOMMU_SUPPORT	y	y

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_IO_STRICT_DEVMEM	N/D	N/D
CONFIG_KEXEC	y	y
CONFIG_KFENCE	n	n
CONFIG_LDISC_AUTOLOAD	n	n
CONFIG_LEGACY_PTYS	n	n
CONFIG_LOCK_DOWN_KERNEL_FORCE_CONFIDENTIALITY	n	n
CONFIG_MODULES	y	y
CONFIG_MODULE_SIG	y	y
CONFIG_MODULE_SIG_ALL	y	y
CONFIG_MODULE_SIG_FORCE	n	n
CONFIG_MODULE_SIG_HASH	sha512	sha512
CONFIG_MODULE_SIG_KEY	certs/signing_key.pem	certs/signing_key.pem
CONFIG_MODULE_SIG_SHA512	y	y
CONFIG_PAGE_POISONING	n	n

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_PAGE_POISONING_NO_SANITY	N/D	N/D
CONFIG_PAGE_POISONING_ZERO	N/D	N/D
CONFIG_PANIC_ON_OOPS	y	y
CONFIG_PANIC_TIMEOUT	0	0
CONFIG_PROC_KCORE	y	y
CONFIG_RANDOMIZE_KSTACK_OFFSET_DEFAULT	n	n
CONFIG_RANDOM_TRUST_BOOTLOADER	y	y
CONFIG_RANDOM_TRUST_CPU	y	y
CONFIG_REFCOUNT_FULL	N/D	N/D
CONFIG_SCHED_CORE	N/D	y
CONFIG_SCHED_STACK_END_CHECK	y	y
CONFIG_SECCOMP	y	y
CONFIG_SECCOMP_FILTER	y	y
CONFIG_SECURITY	y	y
CONFIG_SECURITY_DMESG_RESTRICT	y	y

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SECURITY_LANDLOCK	n	n
CONFIG_SECURITY_LOCKDOWN_LSM	y	y
CONFIG_SECURITY_LOCKDOWN_LSM_EARLY	y	y
CONFIG_SECURITY_SELINUX_BOOTPARAM	y	y
CONFIG_SECURITY_SELINUX_DEVELOP	y	y
CONFIG_SECURITY_SELINUX_DISABLE	n	n
CONFIG_SECURITY_WRITABLE_HOOKS	N/D	N/D
CONFIG_SECURITY_YAMA	y	y
CONFIG_SHUFFLE_PAGE_ALLOCATOR	y	y
CONFIG_SLAB_FREELIST_HARDENED	y	y
CONFIG_SLAB_FREELIST_RANDOM	y	y
CONFIG_SLUB_DEBUG	y	y
CONFIG_STACKPROTECTOR	y	y

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_STACKPROTECTOR_STRONG	y	y
CONFIG_STATIC_USERMODEHELPER	n	n
CONFIG_STRICT_DEVMEM	n	n
CONFIG_STRICT_KERNEL_RWX	y	y
CONFIG_STRICT_MODULE_RWX	y	y
CONFIG_SYN_COOKIES	y	y
CONFIG_VMAP_STACK	y	y
CONFIG_WERROR	n	n
CONFIG_ZERO_CALL_USED_REGS	n	n

Consenti l'inserimento/sostituzione dei metodi ACPI in fase di esecuzione (CONFIG_ACPI_CUSTOM_METHOD)

Amazon Linux disabilita questa opzione in quanto consente agli utenti `root` di scrivere nella memoria kernel arbitraria.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Formati binari vari (**`binfmt_misc`**)

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. In AL2023, questa funzionalità è opzionale ed è sviluppata come modulo del kernel.

Supporto di **BUG()**

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

BUG() se il kernel riscontra un danneggiamento dei dati durante la verifica della validità delle strutture di memoria del kernel

Alcune parti del kernel Linux controllano la coerenza interna delle strutture di dati e possono eseguire `BUG()` quando rilevano un danneggiamento dei dati.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

COMPAT_BRK

Con questa opzione disabilitata (che è il modo in cui Amazon Linux configura il kernel), l'impostazione predefinita per `randomize_va_space sysctl` è 2, che abilita anche la randomizzazione degli heap sulla base `mmap`, sullo stack e sulla randomizzazione delle pagine VDSO.

Questa opzione esiste nel kernel per garantire la compatibilità con alcuni file binari `libc.so.5` obsoleti del 1996 e precedenti.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

COMPAT_VDSO

Questa opzione di configurazione è rilevante per `x86-64` e non per `aarch64`. Impostandola su `n`, il kernel di Amazon Linux non rende visibile un Virtual Dynamic Shared Object (VDSO) a 32 bit a un indirizzo prevedibile. La più recente libreria `glibc` nota per essere danneggiata dall'impostazione di questa opzione su `n` è `glibc` 2.3.3, del 2004.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Rafforzamento riservato **CONFIG_DEBUG**

Le opzioni di configurazione del kernel Linux riservate da `CONFIG_DEBUG` sono in genere progettate per l'uso in kernel creati per problemi di debug, e aspetti come le prestazioni non sono una priorità. AL2023 `CONFIG_DEBUG_LIST` abilita l'opzione di indurimento.

Disabilitazione di DMA per i dispositivi PCI nello stub EFI prima della configurazione di IOMMU

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Rafforzamento per la copia della memoria tra kernel e spazio utente

Quando il kernel deve copiare la memoria da o verso lo spazio utente, questa opzione abilita alcuni controlli che possono proteggere da alcune classi di problemi di overflow dell'heap.

L'opzione `CONFIG_HARDENED_USERCOPY_FALLBACK` esisteva nei kernel da 4.16 a 5.15 per aiutare gli sviluppatori del kernel a scoprire eventuali voci mancanti dell'elenco degli indirizzi consentiti tramite un `WARN()`. Poiché AL2023 fornisce un kernel 6.1, questa opzione non è più rilevante per AL2023.

L'`CONFIG_HARDENED_USERCOPY_PAGESPAN`opzione esisteva nei kernel principalmente come opzione di debug per gli sviluppatori e non si applica più al kernel 6.1 di AL2023.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Supporto per l'ibernazione

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Questa opzione deve essere abilitata per supportare la possibilità di ibernare l'istanza on demand e quella di ibernare le istanze spot interrotte

Generazione di numeri casuali

Il kernel AL2023 è configurato per garantire che sia disponibile un'entropia adeguata per l'utilizzo all'interno di EC2.

`CONFIG_INET_DIAG`

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. In AL2023, questa funzionalità è opzionale ed è sviluppata come modulo del kernel.

Azzeramento di tutta la memoria dell'allocatore di pagine e slab a livello kernel durante l'allocazione e la deallocazione

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Queste opzioni sono disabilitate in AL2023 a causa del possibile impatto sulle prestazioni derivante dall'abilitazione di questa funzionalità per impostazione predefinita. Il comportamento `CONFIG_INIT_ON_ALLOC_DEFAULT_ON` può essere abilitato aggiungendolo `init_on_alloc=1` alla riga di comando del kernel e il comportamento `CONFIG_INIT_ON_FREE_DEFAULT_ON` può essere abilitato aggiungendo `init_on_free=1`.

Inizializzazione di tutte le variabili dello stack su zero (**`CONFIG_INIT_STACK_ALL_ZERO`**)

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Questa opzione richiede GCC versione 12 o successiva, mentre AL2023 viene fornito con GCC 11.

Firma del modulo del kernel

AL2023 firma e convalida le firme dei moduli del kernel. L'opzione `CONFIG_MODULE_SIG_FORCE`, che richiederebbe ai moduli di avere una firma valida, non è abilitata per preservare la compatibilità per gli utenti che creano moduli di terze parti. Per gli utenti che vogliono assicurarsi che tutti i moduli del kernel siano firmati, Modulo di sicurezza Linux (LSM) Lockdown può essere configurato in modo da imporre questa condizione.

`kexec`

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Questa opzione è abilitata in modo da poter utilizzare la funzionalità `kdump`.

Supporto **`IOMMU`**

AL2023 abilita il supporto IOMMU. L'opzione `CONFIG_IOMMU_DEFAULT_DMA_STRICT` non è abilitata per impostazione predefinita, ma questa funzionalità può essere configurata aggiungendo `iommu.passthrough=0 iommu.strict=1` alla riga di comando del kernel.

`kfence`

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Supporto per `pty` legacy

AL2023 utilizza l'interfaccia moderna (). PTY `devpts`

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Modulo di sicurezza Linux (LSM) Lockdown

AL2023 crea l'`lockdown`LSM, che bloccherà automaticamente il kernel quando si utilizza Secure Boot.

L'opzione `CONFIG_LOCK_DOWN_KERNEL_FORCE_CONFIDENTIALITY` non è abilitata. Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Quando non si utilizza Secure Boot, è possibile abilitare l'LSM Lockdown e configurarlo come desiderato.

Poisoning delle pagine

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Analogamente Azzeramento di tutta la memoria dell'allocatore di pagine e slab a livello kernel durante l'allocazione e la deallocazione , questo è disabilitato nel kernel AL2023 a causa del possibile impatto sulle prestazioni.

Stack Protector

Il kernel AL2023 è costruito con la funzionalità di protezione dello stack abilitata con l'opzione. GCC `-fstack-protector-strong`

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

API seccomp BPF

La funzionalità di rafforzamento seccomp viene utilizzata da software come `systemd` e i runtime dei container per rafforzare le applicazioni dello spazio utente.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Timeout **`panic()`**

Il kernel AL2023 è configurato con questo valore impostato su`0`, il che significa che il kernel non si riavvierà in caso di panico. Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. È configurabile tramite `sysctl`, `/proc/sys/kernel/panic` e sulla riga di comando del kernel.

Modelli di sicurezza

AL2023 abilita SELinux in modalità Permissive per impostazione predefinita. Per ulteriori informazioni, consulta Impostazione delle modalità SELinux per AL2023.

Anche i moduli Modulo di sicurezza Linux (LSM) Lockdown e `yama` sono abilitati.

`/proc/kcore`

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Randomizzazione dell'offset dello stack del kernel all'inserimento di syscall

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Questa opzione può essere abilitata impostando `randomize_kstack_offset=on` sulla riga di comando del kernel.

Controlli di conteggio dei riferimenti (**`CONFIG_REFCOUNT_FULL`**)

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Attualmente questa opzione non è abilitata a causa del suo possibile impatto sulle prestazioni.

Consapevolezza del pianificatore dei core SMT (**`CONFIG_SCHED_CORE`**)

Il kernel AL2023 è costruito con`CONFIG_SCHED_CORE`, il che consente l'utilizzo da parte delle applicazioni userspace. `prctl(PR_SCHED_CORE)` Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Verifica della presenza di danneggiamento dello stack durante le chiamate a **`schedule()`** (**`CONFIG_SCHED_STACK_END_CHECK`**)

Il kernel AL2023 è compilato con enabled. `CONFIG_SCHED_STACK_END_CHECK` Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Rafforzamento dell'allocatore di memoria

Il kernel AL2023 consente il rafforzamento dell'allocatore di memoria del kernel con le opzioni, e. `CONFIG_SHUFFLE_PAGE_ALLOCATOR` `CONFIG_SLAB_FREELIST_HARDENED` `CONFIG_SLAB_FREELIST_RANDOM` Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Supporto per il debug SLUB

Il kernel AL2023 abilita `CONFIG_SLUB_DEBUG` poiché questa opzione abilita funzionalità di debug opzionali per l'allocatore che possono essere abilitate sulla riga di comando del kernel. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

CONFIG_STATIC_USERMODEHELPER

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP. Questo perché `CONFIG_STATIC_USERMODEHELPER` richiede un supporto speciale da parte della distribuzione, che attualmente non è presente in Amazon Linux.

Testo del kernel di sola lettura e rodata (**`CONFIG_STRICT_KERNEL_RWX`** e **`CONFIG_STRICT_MODULE_RWX`**)

Il kernel AL2023 è configurato per contrassegnare il testo e la memoria del kernel e dei moduli del kernel come di sola lettura e la rodata memoria non testuale contrassegnata come non eseguibile. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Supporto per TCP syncookie (**`CONFIG_SYN_COOKIES`**)

Il kernel AL2023 è costruito con il supporto per i syncookie TCP. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Stack mappato virtualmente con pagine guard (**CONFIG_VMAP_STACK**)

Il kernel AL2023 è costruito con`CONFIG_VMAP_STACK`, abilita stack di kernel mappati virtualmente con pagine di protezione. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Compilazione tramite avvisi del compilatore come errori (**CONFIG_WERROR**)

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Registrazione dell'azzeramento sulla funzione exit (**CONFIG_ZERO_CALL_USED_REGS**)

Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Indirizzo minimo per l'allocazione dello spazio utente

Questa opzione di rafforzamento può aiutare a ridurre l'impatto dei bug dei puntatori NULL del kernel. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Opzioni di rafforzamento specifiche **clang**

Il kernel AL2023 è costruito con GCC anziché conclang, quindi l'opzione di `CONFIG_CFI_CLANG` hardening non può essere abilitata, il che rende inoltre non applicabile. `CONFIG_CFI_PERMISSIVE` Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Opzioni di rafforzamento del kernel specifiche di x86-64

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_AMD_IOMMU	N/D	y
CONFIG_AMD_IOMMU_V2	N/D	y
CONFIG_IA32_EMULATION	N/D	y

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_INTEL_IOMMU	N/D	y
CONFIG_INTEL_IOMMU_DEFAULT_ON	N/D	n
CONFIG_INTEL_IOMMU_SVM	N/D	n
CONFIG_LEGACY_VSYSCALL_NONE	N/D	n
CONFIG_MODIFY_LDT_SYSCALL	N/D	n
CONFIG_PAGE_TABLE_ISOLATION	N/D	y
CONFIG_RANDOMIZE_MEMORY	N/D	y
CONFIG_X86_64	N/D	y
CONFIG_X86_MSR	N/D	y
CONFIG_X86_VSYSCALL_EMULATION	N/D	y
CONFIG_X86_X32	N/D	N/D
CONFIG_X86_X32_ABI	N/D	n

Supporto per x86-64

Il supporto base per x86-64 include il supporto per i bit Physical Address Extension (PAE) e No eXecute (NX). Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Supporto per IOMMU AMD e Intel

Il kernel AL2023 supporta AMD e Intel. IOMMUs Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

L'opzione `CONFIG_INTEL_IOMMU_DEFAULT_ON` non è impostata, ma può essere abilitata passando `intel_iommu=on` alla riga di comando del kernel. Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

L'`CONFIG_INTEL_IOMMU_SVM`opzione non è attualmente abilitata in AL2023. Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Supporto per lo spazio utente a 32 bit

Important

Il supporto per lo spazio utente x86 a 32 bit è obsoleto e il supporto per l'esecuzione di file binari dello spazio utente a 32 bit potrebbe essere rimosso in una futura versione principale di Amazon Linux.

Note

Sebbene AL2023 non includa più alcun pacchetto a 32 bit, il kernel supporterà comunque l'esecuzione di uno spazio utente a 32 bit. Per ulteriori informazioni, consulta Pacchetti x86 (i686) a 32 bit.

Per supportare l'esecuzione di applicazioni userspace a 32 bit, AL2023 non abilita l'`CONFIG_X86_VSYSCALL_EMULATION`opzione e abilita le opzioni, and. `CONFIG_IA32_EMULATION` `CONFIG_COMPAT` `CONFIG_X86_VSYSCALL_EMULATION` Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

L'ABI x32 nativo a 32 bit per processori a 64 bit non è abilitato (`CONFIG_X86_X32` e `CONFIG_X86_X32_ABI`). Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Supporto per Model Specific Register x86 (MSR)

L'opzione `CONFIG_X86_MSR` è abilitata per supportare `turbostat`. Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

syscall **`modify_ldt`**

AL2023 non consente ai programmi utente di modificare la Local Descriptor Table (LDT) x86 con syscall. `modify_ldt` Questa chiamata è necessaria per eseguire codice a 16 bit o segmentato e la sua assenza può compromettere software come `dosemu`, l'esecuzione di alcuni programmi in WINE e alcune librerie di threading molto vecchie. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Rimozione della mappatura del kernel in modalità utente

AL2023 configura il kernel in modo che la maggior parte degli indirizzi del kernel non sia mappata nello spazio utente. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Randomizzazione delle sezioni di memoria del kernel

AL2023 configura il kernel per randomizzare gli indirizzi virtuali di base delle sezioni di memoria del kernel. Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Opzioni di rafforzamento del kernel specifiche di aarch64

Opzione **`CONFIG`**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
`CONFIG_ARM64_BTI`	y	N/D
`CONFIG_ARM64_BTI_KERNEL`	N/D	N/D
`CONFIG_ARM64_PTR_AUTH`	y	N/D
`CONFIG_ARM64_PTR_AUTH_KERNEL`	y	N/D

Opzione **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_ARM64_SW_TTBR0_PAN	y	N/D
CONFIG_UNMAP_KERNEL_AT_EL0	y	N/D

Identificazione dei target di ramo

Il kernel AL2023 abilita il supporto per Branch Target Identification (). CONFIG_ARM64_BTI Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

L'opzione CONFIG_ARM64_BTI_KERNEL non è abilitata in AL2023 in quanto è stata creata con GCC e il supporto per la creazione del kernel con questa opzione è attualmente disabilitato nel kernel upstream a causa di un bug di gcc. Sebbene questa opzione sia una delle impostazioni consigliate per Kernel Self Protection Project (KSPP), AL2023 non imposta questa opzione di configurazione secondo quanto consigliato da KSPP.

Autenticazione dei puntatori (**CONFIG_ARM64_PTR_AUTH**)

Il kernel AL2023 è costruito con il supporto per l'estensione Pointer Authentication (parte delle estensioni ARMv8.3), che può essere utilizzata per aiutare a mitigare le tecniche di Return Oriented Programming (ROP). Il supporto hardware richiesto per l'autenticazione dei puntatori su Graviton è stato introdotto con Graviton 3.

L'opzione CONFIG_ARM64_PTR_AUTH è abilitata e fornisce supporto per l'autenticazione dei puntatori per lo spazio utente. Poiché anche l'CONFIG_ARM64_PTR_AUTH_KERNELopzione è abilitata, il kernel AL2023 è in grado di utilizzare autonomamente la protezione dell'indirizzo di ritorno.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Emulazione dell'accesso con privilegi che non usa mai lo switching **TTBR0_EL1**

Questa opzione impedisce al kernel di accedere direttamente alla memoria dello spazio utente, con TTBR0_EL1 che viene impostato solo temporaneamente su un valore valido dalle routine di accesso utente.

Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Annullamento della mappatura del kernel durante l'esecuzione nello spazio utente

Il kernel AL2023 è configurato per demappare il kernel quando viene eseguito in userspace (). `CONFIG_UNMAP_KERNEL_AT_EL0` Questa opzione è una delle impostazioni consigliate per Kernel Self Protection Project.

Avvio sicuro UEFI su AL2023

AL2023 supporta UEFI Secure Boot a partire dalla versione 2023.1. Devi utilizzare AL2023 con istanze Amazon EC2 che supportano sia UEFI che UEFI Secure Boot. Per ulteriori informazioni, consulta Avvio di un'istanza nella Guida per l'utente di Amazon EC2 per istanze Linux.

Le istanze AL2023 con UEFI Secure Boot abilitato accettano solo codice a livello di kernel, incluso il kernel Linux e i moduli, che sono firmati da, in Amazon modo da poter garantire che l'istanza esegua solo codici a livello di kernel firmati da. AWS

Per ulteriori informazioni sulle istanze Amazon EC2 e UEFI Secure Boot, consulta UEFI Secure Boot nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Prerequisiti

- Devi utilizzare un'AMI con AL2023 rilascio 2023.1 o successivo.
- Il tipo di istanza deve supportare UEFI Secure Boot. Per ulteriori informazioni, consulta Avvio di un'istanza nella Guida per l'utente di Amazon EC2 per istanze Linux.

Abilita UEFI Secure Boot su AL2023

Le AMI AL2023 standard incorporano un bootloader e un kernel firmati dalle nostre chiavi. Puoi abilitare UEFI Secure Boot registrando le istanze esistenti o creando AMI con UEFI Secure Boot preabilitato mediante registrazione un'immagine da uno snapshot. UEFI Secure Boot non è abilitato per impostazione predefinita sulle AMI AL2023 standard.

La modalità di avvio delle AMI AL2023 è impostata su `uefi-preferred` garantendo così che le istanze avviate con queste AMI usino il firmware UEFI, se il tipo di istanza supporta UEFI. Se il tipo di istanza non supporta UEFI, l'istanza viene avviata con il firmware BIOS legacy. Quando un'istanza viene avviata in modalità BIOS legacy, UEFI Secure Boot non viene applicato.

Per ulteriori informazioni sulle modalità di avvio AMI per le istanze Amazon EC2, consulta la pagina dedicata alle modalità di avvio nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Argomenti

Registrazione di un'istanza esistente

Per registrare un'istanza esistente, compila le variabili specifiche del firmware UEFI con un set di chiavi che consentono al firmware di verificare il bootloader e al bootloader di verificare il kernel all'avvio successivo.

1. Amazon Linux fornisce uno strumento per semplificare il processo di registrazione. Esegui il comando seguente per effettuare il provisioning dell'istanza con il set di chiavi e certificati necessario.

   ```
   sudo amazon-linux-sb enroll
   ```

2. Esegui il seguente comando per riavviare l'istanza. Dopo il riavvio dell'istanza, verrà abilitato UEFI Secure Boot.

   ```
   sudo reboot
   ```

> **Note**
>
> Attualmente le AMI Amazon Linux non supportano Nitro Trusted Platform Module (NitroTPM). Se hai bisogno di NitroTPM oltre a UEFI Secure Boot, usa le informazioni nella sezione seguente.

Registrazione di un'immagine dallo snapshot

Quando registri un'AMI da uno snapshot di un volume root di Amazon EBS utilizzando l'API `register-image` Amazon EC2, puoi effettuare il provisioning dell'AMI con un blob binario che

contiene lo stato dell'archivio di variabili UEFI. Fornendo `UefiData` AL2023, abiliti UEFI Secure Boot e non devi seguire i passaggi della sezione precedente.

Per ulteriori informazioni sulla creazione e l'utilizzo di un blob binario, consulta Opzione B: creazione di un blob binario contenente un archivio delle variabili preriempito nella Guida per l'utente di Amazon EC2 per le istanze Linux.

AL2023 fornisce un blob binario predefinito che può essere utilizzato direttamente sulle istanze Amazon EC2. Il blob binario si trova in `/usr/share/amazon-linux-sb-keys/uefi.vars` su un'istanza in esecuzione. Questo blob è fornito tramite il pacchetto RPM `amazon-linux-sb-keys` che viene installato per impostazione predefinita sulle AMI AL2023 a partire dal rilascio 2023.1.

> **Note**
>
> Per assicurarti di utilizzare la versione più recente delle chiavi e delle revoche, usa il blob dello stesso rilascio di AL2023 che usi per creare l'AMI.

Quando registri un'immagine, si consiglia di utilizzare il parametro `BootMode` dell'API `RegisterImage` impostata su `uefi`. Ciò consente di abilitare NitroTPM impostando il parametro `TpmSupport` su. `v2.0` Inoltre, impostando `BootMode` su `uefi` è possibile garantire che UEFI Secure Boot sia abilitato e non possa essere disabilitato accidentalmente quando si passa a un tipo di istanza che non supporta UEFI.

Per ulteriori informazioni su NitroTPM, consulta la pagina dedicata a NitroTPM nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Aggiornamenti di revoca

Potrebbe essere necessario che Amazon Linux distribuisca una nuova versione del bootloader `grub2` o del kernel Linux firmata con chiavi aggiornate. In tal caso, potrebbe essere necessario revocare la vecchia chiave per evitare la possibilità che bug sfruttabili delle versioni precedenti del bootloader possano aggirare il processo di verifica di UEFI Secure Boot.

Gli aggiornamenti dei pacchetti ai pacchetti `grub2` o `kernel` aggiornano sempre automaticamente l'elenco delle revoche nell'archivio di variabili UEFI dell'istanza in esecuzione. Ciò significa che con UEFI Secure Boot abilitato, non è più possibile eseguire la versione obsoleta di un pacchetto dopo aver installato un aggiornamento di sicurezza per il pacchetto.

Come funziona UEFI Secure Boot su AL2023

A differenza di altre distribuzioni Linux, Amazon Linux non fornisce un componente aggiuntivo, chiamato shim, che funge da bootloader di prima fase. Lo shim è generalmente firmato con chiavi Microsoft. Ad esempio, nelle distribuzioni Linux con shim, lo shim carica il bootloader `grub2` che usa il codice dello shim per verificare il kernel Linux. Inoltre, lo shim mantiene il proprio set di chiavi e revoche nel database Machine Owner Key (MOK) situato nell'archivio di variabili UEFI e controllato con lo strumento `mokutil`.

Amazon Linux non fornisce uno shim. Poiché il proprietario dell'AMI controlla le variabili UEFI, questo passaggio intermedio non è necessario e può influire negativamente sui tempi di avvio e lancio. Inoltre, per impostazione predefinita, abbiamo scelto di non includere l'attendibilità nelle chiavi di tutti i fornitori, per ridurre la possibilità che i file binari indesiderati possano essere eseguiti. Come sempre, i clienti possono includere file binari se lo desiderano.

Con Amazon Linux, UEFI carica e verifica direttamente il nostro bootloader `grub2`. Il bootloader `grub2` è stato modificato per utilizzare UEFI per verificare il kernel Linux dopo averlo caricato. Pertanto, il kernel Linux viene verificato utilizzando gli stessi certificati memorizzati nella normale variabile db UEFI (database delle chiavi autorizzate) e testato rispetto alla stessa variabile `dbx` (database delle revoche) del bootloader e di altri file binari UEFI. Poiché forniamo le nostre chiavi PK e KEK, che controllano l'accesso al database db e al database dbx, possiamo distribuire le revoche e gli aggiornamenti firmati secondo necessità senza un intermediario come lo shim.

Per ulteriori informazioni su UEFI Secure Boot, consulta Come funziona UEFI Secure Boot nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Registrazione di chiavi personalizzate

Come documentato nella sezione precedente, Amazon Linux non richiede uno `shim` per UEFI Secure Boot su Amazon EC2. Quando leggi la documentazione per altre distribuzioni Linux, potresti trovare documentazione per la gestione del database Machine Owner Key (MOK) utilizzando `mokutil`, che non è presente su AL2023. Gli ambienti `shim` e MOK aggirano alcune limitazioni della registrazione delle chiavi nel firmware UEFI che non sono applicabili al modo in cui Amazon EC2 implementa UEFI Secure Boot. Con Amazon EC2 sono disponibili meccanismi per manipolare facilmente e direttamente le chiavi nell'archivio di variabili UEFI.

Se desideri registrare le tue chiavi, puoi farlo manipolando l'archivio delle variabili all'interno di un'istanza esistente (consulta Aggiunta delle chiavi all'archivio delle variabili dall'interno dell'istanza)

o creando un blob binario precompilato (consulta Creazione di un blob binario contenente un archivio delle variabili preriempito).

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.