aws

Guide de l’utilisateur

Amazon Linux 2

Amazon Linux 2: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon Linux 2 ?

Amazon Linux 2 (AL2) est un système d'exploitation Linux développé par Amazon Web Services (AWS). AL2 est conçu pour fournir un environnement stable, sécurisé et performant pour les applications exécutées sur Amazon EC2. Il inclut également des packages permettant une intégration efficaceAWS, notamment des outils de configuration de lancement et de nombreuses AWS bibliothèques et outils populaires. AWSfournit des mises à jour de sécurité et de maintenance continues pour toutes les instances en cours d'exécution AL2. De nombreuses applications développées sur CentOS et des distributions similaires s'exécutent sur. AL2 AL2 est fourni sans frais supplémentaires.

> **Note**
>
> AL2 n'est plus la version actuelle d'Amazon Linux. AL2023 est le successeur de. AL2 Pour plus d'informations, consultez Comparing AL2 and AL2 023 et la liste des modifications de Package apportées à AL2 023 dans le Guide de l'utilisateur AL2023.

> **Note**
>
> AL2 suit de près la version en amont de Firefox Extended Support Release (ESR) et passe à la version ESR suivante dès qu'elle sera disponible. Pour plus d'informations, consultez le calendrier de publication de Firefox ESR et les notes de version de Firefox.

Disponibilité Amazon Linux

AWSfournit AL2 023 AL2, et Amazon Linux 1 (AL1anciennement Amazon Linux AMI). Si vous migrez depuis une autre distribution Linux vers Amazon Linux, nous vous recommandons de migrer vers la version AL2 023.

> **Note**
>
> Le support standard pour AL1 a pris fin le 31 décembre 2020. La phase AL1 de support de maintenance s'est terminée le 31 décembre 2023. Pour plus d'informations sur l' AL1 EOL et

le support de maintenance, consultez le billet de blog Update on Amazon Linux AMI end-of-life.

Pour plus d'informations sur Amazon Linux, consultez AL2023 AL2, et AL1.

Pour les images de conteneur Amazon Linux, consultez Image de conteneur Amazon Linux dans le Guide de l'utilisateur Amazon Elastic Container Registry.

Fonctionnalité obsolète dans AL2

Les sections suivantes décrivent les fonctionnalités prises en charge AL2 et absentes dans la version AL2 023. Il s'agit de fonctionnalités telles que les fonctionnalités et les packages qui sont présents dans le AL2 023 AL2, mais pas dans celui-ci et qui ne seront pas ajoutés au AL2 023. Consultez la AL2 documentation pour savoir pendant combien de temps cette fonctionnalité est prise en charge AL2.

Packages **`compat-`**

Tous les packages AL2 avec le préfixe de `compat-` sont fournis pour assurer la compatibilité binaire avec les anciens binaires qui n'ont pas encore été reconstruits pour les versions modernes du package. Chaque nouvelle version majeure d'Amazon Linux ne reprendra aucun `compat-` package des versions précédentes.

Tous les `compat-` packages d'une version d'Amazon Linux (telle que AL2) sont abandonnés et ne sont pas présents dans la version suivante (telle que AL2 023). Nous recommandons vivement de reconstruire le logiciel en fonction des versions mises à jour des bibliothèques.

Fonctionnalité obsolète abandonnée dans AL1, supprimée dans AL2

Cette section décrit les fonctionnalités disponibles dans AL1 et celles qui ne le sont plus AL2.

> **Note**
>
> Dans le cadre de la phase de support de maintenance de AL1, certains packages avaient une date end-of-life (EOL) antérieure à la EOL de. AL1 Pour plus d'informations, consultez la section Déclarations de support AL1 du Package.

> **Note**
>
> Certaines AL1 fonctionnalités ont été abandonnées dans les versions précédentes. Pour plus d'informations, consultez les notes AL1 de publication.

Rubriques

x86 32 bits (i686) AMIs

Dans le cadre de la version 2014.09 de, AL1 Amazon Linux a annoncé qu'il s'agirait de la dernière version à produire du 32 bits. AMIs Par conséquent, depuis la version 2015.03 de, AL1 Amazon Linux ne prend plus en charge l'exécution du système en mode 32 bits. AL2 offre un support d'exécution limité pour les binaires 32 bits sur des hôtes x86-64 et ne fournit pas de packages de développement permettant de créer de nouveaux binaires 32 bits. AL2023 n'inclut plus aucun package d'espace utilisateur 32 bits. Nous recommandons aux utilisateurs de terminer leur transition vers le code 64 bits avant de migrer vers la version AL2 023.

Si vous devez exécuter des fichiers binaires 32 bits sur AL2 023, il est possible d'utiliser l'espace utilisateur 32 bits depuis un AL2 AL2 conteneur exécuté au-dessus de 023. AL2

`aws-apitools-*`remplacé par AWS CLI

Avant la sortie du AWS CLI en septembre 2013, AWS un ensemble d'utilitaires de ligne de commande étaient disponibles, implémentés dansJava, qui permettaient aux utilisateurs de passer des appels d' EC2API Amazon. Ces outils ont été abandonnés en 2015, et ils sont AWS CLI devenus le moyen préféré d'interagir avec Amazon EC2 APIs depuis la ligne de commande. L'ensemble des utilitaires de ligne de commande inclut les `aws-apitools-*` packages suivants.

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

Le support en amont pour les `aws-apitools-*` packages a pris fin en mars 2017. Malgré l'absence de support en amont, Amazon Linux a continué à fournir certains de ces utilitaires de ligne de

commandeaws-apitools-ec2, notamment pour assurer la rétrocompatibilité aux utilisateurs. AWS CLIIl s'agit d'un outil plus robuste et plus complet que les aws-apitools-* packages car il est activement maintenu et fournit un moyen de tout utiliser AWSAPIs.

Les aws-apitools-* packages sont devenus obsolètes en mars 2017 et ne recevront plus de mises à jour. Tous les utilisateurs de l'un de ces packages doivent migrer vers le AWS CLI dès que possible. Ces packages ne sont pas présents dans AL2 023.

AL1 a également fourni les aws-apitools-rds packages aws-apitools-iam et, qui ont été déconseillés dans AL1 Amazon Linux et qui ne sont plus présents dans Amazon Linux à partir de AL2 maintenant.

systemdremplace **upstart** dans AL2

AL2 a été la première version d'Amazon Linux à utiliser le système systemd d'initialisation, upstart en AL1 le remplaçant. Toute configuration upstart spécifique doit être modifiée dans le cadre de la migration AL1 vers une version plus récente d'Amazon Linux. Il n'est pas possible de l'utiliser systemd sur AL1. Le passage de upstart à ne systemd peut donc être effectué que dans le cadre du passage à une version majeure plus récente d'Amazon Linux, telle que AL2 or AL2 023.

Fonctionnalité déconseillée AL2 et supprimée en 2023 AL2

Cette section décrit les fonctionnalités disponibles dans AL2 AL2 023 et celles qui ne le sont plus.

Rubriques

- Packages x86 (i686) 32 bits
- aws-apitools-*remplacé par AWS CLI
- awslogsobsolète au profit de l'agent Amazon Logs unifié CloudWatch
- bzrsystème de contrôle de révision
- cgroup v1
- log4jhotpatch () log4j-cve-2021-44228-hotpatch
- lsb_release et le package system-lsb-core
- mcrypt
- OpenJDK (7) java-1.7.0-openjdk
- Python 2.7

- rsyslog-opensslremplace rsyslog-gnutls
- Service d'information réseau (NIS)/yp
- Plusieurs noms de domaine dans Amazon VPC create-dhcp-options
- Sun RPC dans glibc
- Empreinte digitale de la clé OpenSSH dans le journal audit
- ld.goldLinker
- ping6
- ftpPackage

Packages x86 (i686) 32 bits

Dans le cadre de la version 2014.09 de AL1, nous avons annoncé qu'il s'agirait de la dernière version à produire du 32 bits. AMIs Par conséquent, à compter de la version 2015.03 de, AL1 Amazon Linux ne prend plus en charge l'exécution du système en mode 32 bits. AL2 fournit un support d'exécution limité pour les binaires 32 bits sur des hôtes x86-64 et ne fournit pas de packages de développement permettant de créer de nouveaux binaires 32 bits. AL2023 n'inclut plus aucun package d'espace utilisateur 32 bits. Nous recommandons aux clients de terminer leur transition vers le code 64 bits.

Si vous devez exécuter des fichiers binaires 32 bits sur AL2 023, il est possible d'utiliser l'espace utilisateur 32 bits depuis un AL2 AL2 conteneur exécuté au-dessus de 023. AL2

`aws-apitools-*`remplacé par AWS CLI

Avant la sortie du AWS CLI en septembre 2013, AWS a mis à disposition un ensemble d'utilitaires de ligne de commande, implémentés dansJava, qui permettaient aux clients de passer des appels d' EC2API Amazon. Ces outils ont été déconseillés en 2015, et ils sont AWS CLI devenus le moyen préféré d'interagir avec Amazon EC2 APIs depuis la ligne de commande. Cela inclut les `aws-apitools-*` packages suivants.

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

Le support en amont pour les `aws-apitools-*` packages a pris fin en mars 2017. Malgré l'absence de support en amont, Amazon Linux a continué à fournir certains de ces utilitaires de ligne de commande (tels que`aws-apitools-ec2`) afin de fournir une rétrocompatibilité aux clients. AWS CLIIl s'agit d'un outil plus robuste et plus complet que les `aws-apitools-*` packages car il est activement maintenu et fournit un moyen de tout utiliser AWSAPIs.

Les `aws-apitools-*` packages sont devenus obsolètes en mars 2017 et ne recevront plus de mises à jour. Tous les utilisateurs de l'un de ces packages doivent migrer vers le AWS CLI dès que possible. Ces packages ne sont pas présents dans AL2 023.

`awslogs`obsolète au profit de l'agent Amazon Logs unifié CloudWatch

Le `awslogs`package est obsolète AL2 et n'est plus présent dans AL2 023. Il est remplacé par l'agent Unified CloudWatch Logs, disponible dans le `amazon-cloudwatch-agent` package. Pour plus d'informations, consultez le guide de l'utilisateur Amazon CloudWatch Logs.

`bzr`système de contrôle de révision

Le système de contrôle des révisions GNU Bazaar(`bzr`) est abandonné AL2 et n'est plus présent en AL2 023.

Il est `bzr` conseillé aux utilisateurs de migrer leurs référentiels vers`git`.

cgroup v1

AL2023 passe à la hiérarchie des groupes de contrôle unifiés (cgroup v2), alors qu'il AL2 utilise cgroup v1. Comme cgroup v2 AL2 n'est pas compatible, cette migration doit être terminée dans le cadre du passage à la version AL2 023.

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

> **Note**
>
> Le `log4j-cve-2021-44228-hotpatch` package est obsolète AL2 et supprimé en AL2 023.

En réponse à CVE-2021-44228, Amazon Linux a publié une version empaquetée RPM du Hotpatch pour Apache Log4j pour et. AL1 AL2 Dans l'annonce de l'ajout du hotpatch à Amazon Linux, nous

avons noté que « l'installation du hotpatch ne remplace pas la mise à jour vers une version de log4j qui atténue le CVE-2021-44228 ou le CVE-2021-45046 ».

La mise à jour corrective à chaud était une mesure d'atténuation permettant de laisser le temps nécessaire au correctif `log4j`. La première version de disponibilité générale de AL2 023 a eu lieu 15 mois après CVE-2021-44228. La version AL2 023 n'est donc pas livrée avec le hotpatch (activé ou non).

Il est conseillé aux clients qui exécutent leurs propres versions `log4j` sur Amazon Linux de s'assurer qu'ils ont effectué une mise à jour vers des versions non affectées par les CVE-2021-44228 et les CVE-2021-45046.

`lsb_release` et le package `system-lsb-core`

Historiquement, certains logiciels `lsb_release` appelaient la commande (AL2 fournie dans le `system-lsb-core` package) pour obtenir des informations sur la distribution Linux sur laquelle elle était exécutée. Le projet Linux Standards Base (LSB) a introduit cette commande et les distributions Linux l'ont adoptée. Les distributions Linux ont évolué pour utiliser le standard simplifié consistant à conserver ces informations dans `/etc/os-release` et d'autres fichiers connexes.

Le standard `os-release` est issu de `systemd`. Pour plus d'informations, consultez la documentation systemd sur os-release (langue française non garantie).

AL2023 n'est pas livré avec la `lsb_release` commande et n'inclut pas le `system-lsb-core` package. Le logiciel doit terminer la transition vers le standard `os-release` pour maintenir la compatibilité avec Amazon Linux et les autres distributions majeures de Linux.

`mcrypt`

La `mcrypt` bibliothèque et l'PHPextension associée sont devenues obsolètes en AL2 023 et ne sont plus présentes AL2.

Upstream a rendu l'`mcrypt`extension PHP obsolète dans la PHP version 7.1, qui a été publiée pour la première fois en décembre 2016 et dont la version finale a été publiée en octobre 2019.

La `mcrypt` bibliothèque en amont a été publiée pour la dernière fois en 2007 et n'a pas effectué la migration depuis le contrôle des `cvs` révisions SourceForge requise pour les nouveaux commits en 2017, le commit le plus récent (et seulement pour les 3 années précédentes) datant de 2011, supprimant la mention du projet ayant un mainteneur.

Il est conseillé à tous `mcrypt` les utilisateurs restants de porter leur code versOpenSSL, car il ne `mcrypt` sera pas ajouté à AL2 023.

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

> **Note**
>
> AL2023 fournit plusieurs versions d'Amazon Corretto pour prendre en charge les charges de travail basées. Java Les packages OpenJDK 7 sont obsolètes et ne sont plus présents AL2 dans 023. AL2 Le plus ancien JDK disponible en AL2 2003 est fourni par Corretto 8.

Pour plus d'informations sur Java sur Amazon Linux, consultezJavadans AL2.

Python 2.7

> **Note**
>
> AL2023 a supprimé Python 2.7, de sorte que tous les composants du système d'exploitation nécessitant Python sont écrits pour fonctionner avec Python 3. Pour continuer à utiliser une version de Python fournie et prise en charge par Amazon Linux, convertissez le code Python 2 en code pour Python 3.

Pour plus d'informations sur Python sur Amazon Linux, consultezPythondans AL2.

`rsyslog-openssl`remplace **`rsyslog-gnutls`**

Le `rsyslog-gnutls` package est obsolète et n'est plus présent dans AL2 023. AL2 Le `rsyslog-openssl` colis doit être un remplacement direct pour toute utilisation du `rsyslog-gnutls` package.

Service d'information réseau (NIS)/**`yp`**

Le Network Information Service (NIS), initialement appelé Pages Jaunes ou YP obsolète depuis 2003 AL2, n'existe plus depuis 023. AL2 Cela inclut les packages suivants : `ypbind`, `ypserv`, et`yp-tools`. Cette fonctionnalité a été supprimée dans NIS les autres packages intégrés dans la version AL2 023.

Plusieurs noms de domaine dans Amazon VPC `create-dhcp-options`

Dans Amazon Linux 2, il était possible de transmettre plusieurs noms de domaine dans le `domain-name` paramètre à `create-dhcp-options`, ce qui aurait pour résultat de `/etc/resolv.conf` contenir quelque chose comme`search foo.example.com bar.example.com`. Le DHCP serveur Amazon VPC envoie la liste des noms de domaine fournis à l'aide de l'DHCPoption 15, qui ne prend en charge qu'un seul nom de domaine (voir la section 3.17 de la RFC 2132). Étant donné que AL2 023 utilise `systemd-networkd` pour la configuration réseau, qui suit leRFC, cette fonctionnalité accidentelle n' AL2 est pas présente le AL2 023

Voici ce que dit la AWS CLIdocumentation Amazon VPC : « Certains systèmes d'exploitation Linux acceptent plusieurs noms de domaine séparés par des espaces. Cependant, Windows d'autres systèmes d'exploitation Linux traitent la valeur comme un domaine unique, ce qui entraîne un comportement inattendu. Si votre ensemble d'DHCPoptions est associé à un Amazon VPC doté d'instances exécutant des systèmes d'exploitation qui traitent la valeur comme un domaine unique, spécifiez un seul nom de domaine. «

Sur ces systèmes, tels que AL2 023, spécifiez deux domaines à l'aide de l'DHCPoption 15 (qui n'en autorise qu'un), et comme le caractère d'espace n'est pas valide dans les noms de domaine, le caractère d'espace sera codé comme tel`032`, ce qui se traduira par un `/etc/resolv.conf` contenant`search foo.exmple.com032bar.example.com`.

Afin de prendre en charge plusieurs noms de domaine, un DHCP serveur doit utiliser l'DHCPoption 119 (voir RFC 3397, section 2). Consultez le guide de l'utilisateur Amazon VPC pour savoir si cela est pris en charge par le serveur Amazon VPC. DHCP

Sun RPC dans `glibc`

L'implémentation de Sun RPC in `glibc` est obsolète AL2 et supprimée en AL2 023. Il est conseillé aux clients de passer à l'utilisation de la `libtirpc` bibliothèque (disponible dans AL2 et AL2 023) si une Sun RPC fonctionnalité est requise. L'adoption permet `libtirpc` également aux applications de prendre en chargeIPv6.

Ce changement reflète l'adoption par la communauté au sens large de la `glibc` suppression en amont de cette fonctionnalité, par exemple la suppression des Sun RPC interfaces `glibc` dans Fedora et un changement similaire dans Gentoo.

Empreinte digitale de la clé OpenSSH dans le journal **`audit`**

Plus tard dans le cycle de vie de AL2, un correctif a été ajouté au package OpenSSH pour émettre l'empreinte digitale utilisée pour l'authentification. Cette fonctionnalité n'est pas présente dans la version AL2 023.

`ld.gold`Linker

L'`ld.gold`éditeur de liens est disponible dans AL2 et est supprimé dans AL2 023. Les clients qui créent un logiciel qui fait explicitement référence à l'goldéditeur de liens doivent migrer vers l'éditeur de liens normal (`ld.bfd`).

Les notes de publication de GNU Binutils en amont pour la version 2.44 (publiées en février 2025) font état de la suppression de `ld.gold` : « Contrairement à notre pratique précédente, dans cette version, l'archive tar binutils-2.44.tar ne contient pas les sources de l'éditeur de liens Gold. En effet, le gold linker est désormais obsolète et sera finalement supprimé à moins que des volontaires ne se présentent et ne proposent de poursuivre le développement et la maintenance. »

ping6

Dans la AL2 version 023, l'`ping`utilitaire standard est pris en charge de manière native IPv6, et l'utilitaire séparé n'`/bin/ping6`est plus nécessaire. Dans AL2 023, `/usr/sbin/ping6` il s'agit d'un lien symbolique vers l'`/usr/bin/ping`exécutable.

Ce changement fait suite à l'adoption par l'ensemble de la communauté de nouvelles `iputils` versions qui fournissent cette fonctionnalité, par exemple le IPv6 changement de ping dans Fedora.

`ftp`Package

Le `ftp` package n' AL2 est plus disponible dans Amazon Linux à partir de AL2 023. Cette décision a été prise dans le cadre de notre engagement continu en faveur de la sécurité, de la maintenabilité et des pratiques modernes de développement de logiciels. Dans le cadre (ou avant) de la migration vers AL2 023, nous vous recommandons de migrer toute utilisation de l'ancien `ftp` package vers l'une de ses alternatives.

Contexte

L'ancien `ftp` package n'a pas été activement maintenu en amont depuis de nombreuses années. La dernière mise à jour significative du code source a eu lieu au début des années 2000, et le

référentiel source d'origine n'est plus disponible. Bien que certaines distributions Linux aient intégré des correctifs pour corriger des failles de sécurité, la base de code reste largement mal entretenue.

Solutions de remplacement recommandées

AL2023 propose plusieurs alternatives modernes et activement maintenues pour les fonctionnalités FTP :

`lftp`(disponible en AL2 023 AL2 et 2018)

Un programme de transfert de fichiers sophistiqué prenant en charge les protocoles FTP, HTTP, SFTP et autres. Il offre plus de fonctionnalités que le `ftp` client traditionnel et est activement maintenu.

Installation avec : dnf install lftp

`curl`(disponible en AL2 023 AL2 et 2018)

Un outil de ligne de commande polyvalent pour transférer des données avec FTP URLs, FTPS, HTTP, HTTPS et de nombreux autres protocoles.

Disponible par défaut en AL2 2023 via le `curl-minimal` package. Pour une prise en charge plus étendue des protocoles, vous pouvez éventuellement passer à `curl-full` l'utilisation dednf swap curl-minimal curl-full.

`wget`(disponible en AL2 023 AL2 et 2018)

Utilitaire de ligne de commande non interactif permettant de télécharger des fichiers depuis le Web, compatible avec les protocoles HTTP, HTTPS et FTP.

Installation avec : dnf install wget (non installé par défaut dans toutes les images AL2 023)

`sftp`(disponible en AL2 023 AL2 et 2018)

Protocole de transfert de fichiers sécurisé qui fonctionne via SSH et fournit des transferts de fichiers cryptés.

Disponible par défaut dans le cadre du package OpenSSH.

Considérations concernant la migration

Si vos applications ou scripts dépendent de l'ancien `ftp` client, envisagez les approches de migration suivantes :

1. Mettez à jour les scripts pour utiliser des alternatives modernes : modifiez vos scripts pour utiliser `lftpcurl`,`wget`, ou à la `sftp` place de l'ancien `ftp` client.
2. Vérifiez les dépendances des packages : certaines applications peuvent répertorier le `ftp` package en tant que dépendance dans leurs métadonnées de package, même si elles ont depuis longtemps migré vers l'utilisation de protocoles modernes en interne. Dans ces cas, l'application peut fonctionner correctement le AL2 023 malgré l'absence `/usr/bin/ftp` du `ftp` package. Passez en revue les exigences réelles de votre application plutôt que de vous fier uniquement aux dépendances indiquées.
3. Mettre à jour les dépendances des applications : pour les applications que vous gérez et qui déclarent toujours une dépendance au `ftp` package mais ne l'utilisent pas réellement, mettez à jour les métadonnées du package pour supprimer cette dépendance inutile.

Considérations de sécurité

Le protocole FTP transmet les données, y compris les informations d'authentification, en texte clair. Pour les applications sensibles à la sécurité, nous recommandons vivement d'utiliser des alternatives cryptées telles que SFTP ou HTTPS, qui sont prises en charge par les outils alternatifs recommandés.

Préparez votre migration vers AL2 023

Vous pouvez préparer votre passage au AL2 023 pendant que vous continuez à l'utiliser AL2.

Rubriques

Consultez la liste des modifications apportées en AL2 2023

La documentation AL2 023 contient une liste détaillée des modifications mises en œuvre depuis AL2. Ces informations se trouvent dans la section Comparaison AL2 et AL2 023. Vous trouverez également une liste complète des modifications apportées aux packages logiciels dans la section Modifications apportées aux packages dans la AL2 version 023.

AL2023 n'inclut `amazon-linux-extras` pas. Au lieu de cela, il fournit des packages avec espace de noms dans lesquels plusieurs versions sont fournies. Étant donné que de nombreux packages sont mis à jour dans la version AL2 023, les versions de base de la version AL2 023 peuvent être ultérieures aux versions que vous obtenez. `amazon-linux-extras`

> **Note**
>
> Nous vous recommandons de ne pas l'exécuter`amazon-linux-extras`, car c'est une fin de vie.

Après avoir examiné ces sections dans la documentation, vous pouvez déterminer si des modifications apportées à la AL2 version 023 pourraient vous obliger à adapter votre environnement pour la migration. Par exemple, vous devrez peut-être enfin migrer un script Python 2.7 vers Python 3.

Migrer des jobs vers **`systemd`** des minuteries **`cron`**

Par défaut, n'`cron`est pas installé dans AL2 023. Vous pouvez migrer vos `cron` tâches vers `systemd` des minuteries AL2 en vue de la migration vers AL2 023. `systemd`présente de nombreux

avantages, tels qu'un contrôle plus précis du moment où les minuteries sont exécutées et une meilleure journalisation.

AL2 Limites

Les rubriques suivantes traitent des différentes limitations d' AL2Amazon Linux et indiquent si elles ont été résolues dans une version plus récente d'Amazon Linux.

Rubriques

`yum`Impossible de vérifier les signatures GPG créées avec des sous-clés GPG

La version du gestionnaire de `rpm` packages date d'avant l'`rpm`ajout de la prise en AL2 charge de la vérification des signatures de packages effectuées avec des sous-clés GPG. Si vous créez des packages compatibles AL2, vous devez vous assurer d'utiliser des clés de signature GPG compatibles avec celles `rpm` qui font partie de AL2

Afin de garantir la rétrocompatibilité pour les utilisateurs existants, la version de `rpm` in ne AL2 reçoit que des rétroportages de sécurité.

La version d'`rpm`in AL2 023 inclut la prise en charge de la vérification des signatures de packages créées avec des sous-clés GPG.

Comparez AL1 et AL2

Les rubriques suivantes décrivent les principales différences entre AL1 et AL2. Ils contiennent également des informations sur la durée de vie et le support, ainsi que sur les modifications apportées aux packages.

Rubriques

AL1 support et EOL

AL1 est désormais EOL. AL1 a mis fin au support standard le 31 décembre 2020 et était en phase de support de maintenance jusqu'au 31 décembre 2023.

Nous vous recommandons de passer à la dernière version d'Amazon Linux.

Support pour les AWS processeurs Graviton

AL2 a introduit le support pour les processeurs Graviton. AL2Le 023 est encore optimisé pour les processeurs Graviton.

`systemd` remplace **`upstart`** en tant que système **`init`**

Dans AL2, `systemd` remplacé `upstart` en tant que `init` système.

Python 2.6 et 2.7 ont été remplacés par Python 3

Bien que Python 2.6 ait AL1 été marqué comme EOL dans la version 2018.03, les packages étaient toujours dans les référentiels à installer. AL2 livré avec Python 2.7 en tant que première version de Python prise en charge.

AL2023 termine la transition vers Python 3, et aucune version de Python 2.x n'est incluse dans les référentiels.

Comparaison des packages installés sur AL1 et AL2 AMIs

Package	AL1 AMI	AL2 AMI
GeoIP		1.5.0
PyYAML		3,10
acl	2,2,49	2,2,51
acpid	2,0,19	2,0,19
alsa-lib	1,0,22	
amazon-linux-extras		2.0.3
amazon-linux-extras-yum-plugin		2.0.3
amazon-ssm-agent	3,2.1705,0	3,2.1705,0
à	3.1.10	3,113
attr	2,4,46	2,4,46
audit	2.6.5	2.8.1
audit-libs	2.6.5	2.8.1
authconfig	6.2.8	6.2.8
aws-amitools-ec2	1.5,13	
aws-cfn-bootstrap	1.4	2.0
aws-cli	1,18,107	

Package	AL1 AMI	AL2 AMI
awscli		1,18,147
basesystem	10,0	10,0
bash	4,2,46	4,2,46
bash-completion		2.1
bc	1,06,95	1,06,95
bind-export-libs		9,11.4
bind-libs	9.8.2	9,11.4
bind-libs-lite		9,11.4
bind-license		9,11.4
bind-utils	9.8.2	9,11.4
binutils	2,27	2,29.1
blktrace		1.0.5
boost-date-time		1,53,0
boost-system		1,53,0
boost-thread		1,53,0
bridge-utils		1.5
bzip2	1.0.6	1.0.6
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023,2,62	2023,2,62
checkpolicy	2.1.10	

Package	AL1 AMI	AL2 AMI
chkconfig	1.3.49,3	1.7.4
chrony		4.2
cloud-disk-utils	0,27	
cloud-init	0,7,6	19,3
cloud-utils-growpart		0,31
copy-jdk-configs	3.3	
coreutils	8,22	8,22
cpio	2.10	2,12
cracklib	2.8,16	2.9.0
cracklib-dicts	2.8,16	2.9.0
cronie	1.4.4	1.4.11
cronie-anacron	1.4.4	1.4.11
crontabs	1.10	1.11
cryptsetup	1.6.7	1.7.4
cryptsetup-libs	1.6.7	1.7.4
curl	7,61,1	8.3.0
cyrus-sasl	2.1.23	
cyrus-sasl-lib	2.1.23	2.1.26
cyrus-sasl-plain	2.1.23	2.1.26
dash	0,5.5.1	

Package	AL1 AMI	AL2 AMI
db4	4,7,25	
db4-utils	4,7,25	
dbus	1.6,12	1,1,24
dbus-libs	1.6,12	1,1,24
dejavu-fonts-common	2,33	
dejavu-sans-fonts	2,33	
dejavu-serif-fonts	2,33	
device-mapper	1,02,135	1,02,170
device-mapper-event	1,02,135	1,02,170
device-mapper-event-libs	1,02,135	1,02,170
device-mapper-libs	1,02,135	1,02,170
device-mapper-persistent-data	0,6.3	0.7.3
dhclient	4.1.1	4.2.5
dhcp-common	4.1.1	4.2.5
dhcp-libs		4.2.5
diffutils	3.3	3.3
dmidecode		3.2
dmraid	1.0.0.rc16	1.0.0.rc16
dmraid-events	1.0.0.rc16	1.0.0.rc16
dosfstools		3,0,20

Package	AL1 AMI	AL2 AMI
dracut	004	033
dracut-config-ec2		2.0
dracut-config-generic		033
dracut-modules-growroot	0.20	
dump	0.4	
dyninst		9.3.1
e2fsprogs	1,43,5	1,42,9
e2fsprogs-libs	1,43,5	1,42,9
ec2-hibinit-agent	1.0.0	1.0.2
ec2-instance-connect		1.1
ec2- instance-connect-selinux		1.1
ec2-net-utils	0.7	1.7.3
ec2-utils	0.7	1.2
ed	1.1	1.9
elfutils-default-yama-scope		0,176
elfutils-libelf	0,168	0,176
elfutils-libs		0,176
epel-release	6	
ethtool	3,15	4.8
expat	2.1.0	2.1.0

Package	AL1 AMI	AL2 AMI
dans le fichier	5,37	5,11
file-libs	5,37	5,11
filesystem	2,4,30	3.2
findutils	4.4.2	4.5.11
fipscheck	1.3.1	1.4.1
fipscheck-lib	1.3.1	1.4.1
fontconfig	2.8.0	
fontpackages-filesystem	1,41	
freetype	2.3.11	2,8
fuse-libs	2.9.4	2.9.2
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
gdisk	0,8,10	0,8,10
generic-logos	17,0,0	18.0.0
get_reference_source	1.2	
gettext		0,19,8.1
gettext-libs		0,19,8.1
giflib	4.1.6	
glib2	2,36.3	2,56.1
glibc	2,17	2,26

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

Package	AL1 AMI	AL2 AMI
gssproxy		0.7.0
gzip	1.5	1.5
hardlink		1.3
hesiod	3.1.0	
hibagent	1.0.0	1.1.0
hmaccalc	0,9,12	
hostname		3.13
hunspell		1.3.2
hunspell-en		0,20121024
hunspell-en-GB		0,20121024
hunspell-en-US		0,20121024
hwdata	0,233	0,252
info	5.1	5.1
initscripts	9,03,58	9,49,47
iproute	4.4.0	5.10.0
iptables	1.4,21	1.8.4
iptables-libs		1.8.4
iputils	20121221	20180629
irqbalance	1.5.0	1.7.0
jansson		2.10

Package	AL1 AMI	AL2 AMI
java-1.7.0-openjdk	1,7,0,321	
javapackages-tools	0.9.1	
jbigkit-libs		2.0
jpackage-utils	1,7.5	
json-c		0,11
kbd	1.15	1,1,5
kbd-legacy		1,1,5
kbd-misc	1.15	1,1,5
kernel	4,1,4326	5,10199
kernel-tools	4,1,4326	5,10199
keyutils	1.5.8	1.5.8
keyutils-libs	1.5.8	1.5.8
kmod	14	25
kmod-libs	14	25
kpartx	0,4.9	0,4.9
kpatch-runtime		0.9.4
krb5-libs	1.15.1	1.15.1
langtable		0.0.31
langtable-data		0.0.31
langtable-python		0.0.31

Package	AL1 AMI	AL2 AMI
lcms2	2.6	
moins	436	458
libICE	1.0.6	
libSM	1.2.1	
libX11	1.6.0	
libX11-common	1.6.0	
libXau	1.0.6	
libXcomposite	0,4.3	
libXext	1.3.2	
libXfont	1.4.5	
libXi	1.7.2	
libXrender	0,9,8	
libXtst	1.2.2	
libacl	2,2,49	2,2,51
libaio	0,3,109	0,3,109
libassuan	2.0.3	2.1.0
libattr	2,4,46	2,4,46
libbasicobjects		0,11
libblkid	2.23.2	2,30,2
libcap	2,16	2,54

Package	AL1 AMI	AL2 AMI
libcap-ng	0,7,5	0,7,5
libcap54	2,54	
libcgroup	0,40 .rc1	
libcollection		0.7.0
libcom_err	1,43,5	1,42,9
libconfig		1.4.9
libcroco		0,6,12
libcrypt		2,26
libcurl	7,61,1	8.3.0
libdaemon		0,14
libdb		5.3.21
libdb-utils		5.3.21
libdrm		2,4,97
libdwarf		20130207
libedit	2.11	3.0
libestr		0,19
libevent	2,0,21	2,0,21
libfastjson		0,99,4
libfdisk		2,30,2
libffi	3,0,13	3,0,13

Package	AL1 AMI	AL2 AMI
libfontenc	1.0.5	
libgcc		7.3.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgomp		7.3.1
libgpg-error	1.11	1.12
libgssglue	0.1	
libicu	50,2	50,2
libidn	1,18	1,28
libidn2	2.3.0	2.3.0
libini_config		1.3.1
libjpeg-turbo	1,2,90	2,0,90
libmetalink		0,13
libmnl	1.0.3	1.0.3
libmount	2.23.2	2,30,2
libnetfilter_conntrack	1.0.4	1.0.6
libnfnetlink	1.0.1	1.0.1
libnfsidmap	0.25	0.25
libnghttp2	1,33,0	1,41,0
libnih	1.0.1	

Package	AL1 AMI	AL2 AMI
libnl	1.1.4	
libnl3		3,2,28
libnl3-cli		3,2,28
libpath_utils		0,2.1
libpcap		1.5.3
libpciaccess		0,14
libpipeline	1.2.3	1.2.3
libpng	1,2,49	1.5,13
libpsl	0.6.2	
libpwquality	1.2.3	1.2.3
libref_array		0,15
libseccomp		2.4.1
libselinux	2.1.10	2,5
libselinux-utils	2.1.10	2,5
libsemanage	2.1.6	2,5
libsepol	2.1.7	2,5
libsmartcols	2.23.2	2,30,2
libss	1,43,5	1,42,9
libssh2	1.4.2	1.4.3
libsss_idmap		1,1,5

Package	AL1 AMI	AL2 AMI
libsss_nss_idmap		1,1,5
libstdc++		7.3.1
libstdc++72	7.2.1	
libstoragemgmt		1.6.1
libstoragemgmt-python		1.6.1
libstoragemgmt-python-clibs		1.6.1
libsysfs	2.1.0	2.1.0
libtasn1	2.3	4,10
libteam		1,27
libtiff		4.0.3
libtirpc	0,2.4	0,2.4
libudev	173	
libunistring	0.9.3	0.9.3
libuser	0,60	0,60
libutempter	1.1.5	1.1.6
libuuid	2.23.2	2,30,2
libverto	0,2,5	0,2,5
libverto-libevent		0,2,5
libwebp		0.3.0
libxcb	1.11	

Package	AL1 AMI	AL2 AMI
libxml2	2.9.1	2.9.1
libxml2-python		2.9.1
libxml2-python27	2.9.1	
libxslt	1.1.28	
libyaml	0,16	0,14
lm_sensors-libs		3.4.0
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3.7.8	3,8.6
lsof	4,82	4,87
lua	5.1.4	5.1.4
lvm2	2,02,166	2,02,187
lvm2-libs	2,02,166	2,02,187
lz4		1,7.5
mailcap	2.1.31	
make	3,82	3,82
man-db	2.6.3	2.6.3
man-pages	4,10	3,53
man-pages-overrides		7.5.2
mariadb-libs		5,5,68
mdadm	3.2.6	4.0

Package	AL1 AMI	AL2 AMI
microcode_ctl	2.1	2.1
mingetty	1,08	
mlocate		0,26
mtr		0.92
nano	2.5.3	2,9,8
nc	1,84	
ncurses	5.7	6.0
ncurses-base	5.7	6.0
ncurses-libs	5.7	6.0
net-tools	1,60	2.0
nettle		2.7.1
newt	0,52,11	0,52,15
newt-python		0,52,15
newt-python27	0,52,11	
nfs-utils	1.3.0	1.3.0
nspr	4,25,0	4,35,0
nss	3,53,1	3,90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3,53,1	3,90,0
nss-softokn-freebl	3,53,1	3,90,0

Package	AL1 AMI	AL2 AMI
nss-sysinit	3,53,1	3,90,0
nss-tools	3,53,1	3,90,0
nss-util	3,53,1	3,90,0
ntp	4,2,8 p15	
ntpdate	4,2,8 p15	
ntsysv	1.3.49,3	1.7.4
numactl	2.0.7	
numactl-libs		2.0.9
openldap	2,4,40	2,4,44
openssh	7,4 p1	7,4 p1
openssh-clients	7,4 p1	7,4 p1
openssh-server	7,4 p1	7,4 p1
openssl	1,02k	1,02k
openssl-libs		1,02k
os-prober		1.58
p11-kit	0,18,5	0,23,22
p11-kit-trust	0,18,5	0,23,22
pam	1.1.8	1.1.8
pam_ccreds	10	
pam_krb5	2.3.11	

Package	AL1 AMI	AL2 AMI
pam_passwdqc	1.0.5	
parted	2.1	3.1
passwd	0,79	0,79
pciutils	3.1.10	3.5.1
pciutils-libs	3.1.10	3.5.1
pcre	8,21	8,32
pcre2		10,23
perl	5.16,3	5.16,3
perl-Carp	1,26	1,26
perl-Digest	1,17	
perl-Digest-HMAC	1,03	
Perl-Digest- MD5	2,52	
perl-Digest-SHA	5,85	
perl-Encode	2,51	2,51
perl-Exporter	5,68	5,68
perl-File-Path	2,09	2,09
perl-File-Temp	0,23,01	0,23,01
perl-Filter	1,49	1,49
perl-Getopt-Long	2,40	2,40
perl-HTTP-Tiny	0,033	0,033

Package	AL1 AMI	AL2 AMI
perl- PathTools	3,40	3,40
perl-Pod-Escapes	1.04	1.04
perl-Pod-Perldoc	3,20	3,20
perl-Pod-Simple	3,28	3,28
perl-Pod-Usage	1,63	1,63
perl-Scalar-List-Utils	1,27	1,27
perl-Socket	2,010	2,010
perl-Storable	2,45	2,45
Texte Perl- ParseWords	3,29	3,29
Heure Perl- HiRes	1,9725	1,9725
perl-Time-Local	1,2300	1,2300
perl-constant	1,27	1,27
perl-libs	5.16,3	5.16,3
perl-macros	5.16,3	5.16,3
perl-parent	0,225	0,225
perl-podlators	2.5.1	2.5.1
perl-threads	1,87	1,87
perl-threads-shared	1,43	1,43
pinentry	0,7,6	0.8.1
pkgconfig	0,27,1	0,27,1

Package	AL1 AMI	AL2 AMI
plymouth		0,8.9
plymouth-core-libs		0,8.9
plymouth-scripts		0,8.9
pm-utils	1.4.1	1.4.1
policycoreutils	2.1.12	2,5
popt	1.13	1.13
postfix		2.10.1
procmail	3,22	
procps	3.2.8	
procps-ng		3.3.10
psacct	6.3.2	6.6.1
psmisc	22,20	22,20
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0,5.3
pystache		0,5.3
python		2.7,18
python-babel		0.9.6
python-backports		1.0
python-backports-ssl_match_hostname		3.5.0.1

Package	AL1 AMI	AL2 AMI
python-cffi		1.6.0
python-chardet		2.2.1
python-configobj		4.7.2
python-daemon		1.6
python-devel		2.7,18
python-docutils		0,12
python-enum34		1.0.4
python-idna		2,4
python-iniparse		0.4
python-ipaddress		1,0,16
python-jinja2		2.7.2
python-jsonpatch		1.2
python-jsonpointer		1.9
python-jwcrypto		0,4.2
python-kitchen		1.1.1
python-libs		2.7,18
python-lockfile		0.9.1
python-markupsafe		0,11
python-pillow		2.0.0
python-ply		3.4

Package	AL1 AMI	AL2 AMI
python-pycparser		2.14
python-pycurl		7,19,0
python-repoze-lru		0.4
python-requests		2.6.0
python-simplejson		3.2.0
python-urlgrabber		3,10
python-urllib3		1,25,9
python2-botocore		1,18,6
python2-colorama		0,3,9
python2-cryptography		1.7.2
python2-dateutil		2.6.1
python2-futures		3.0.5
python2-jmespath		0.9.3
python2-jsonschema		2.5.1
python2-oauthlib		2.0.1
python2-pyasn1		0,19
python2-rpm		4.11.3
python2-rsa		3.4.1
python2-s3transfer		0,3.3
python2-setuptools		41,2,0

Package	AL1 AMI	AL2 AMI
python2-six		1.11.0
python27	2.7,18	
python27-PyYAML	3,10	
python27-babel	0.9.4	
python27-backports	1.0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-boto	2,48,0	
python27-botocore	1,1,31	
python27-chardet	2.0.1	
python27-colorama	0,4.1	
python27-configobj	4.7.2	
python27-crypto	2.6.1	
python27-daemon	1.5.2	
python27-dateutil	2.1	
python27-devel	2.7,18	
python27-docutils	0,11	
python27-ecdsa	0,11	
python27-futures	3.0.3	
python27-imaging	1.1.6	
python27-iniparse	0,3.1	

Package	AL1 AMI	AL2 AMI
python27-jinja2	2.7.2	
python27-jmespath	0.9.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1.0	
python27-kitchen	1.1.1	
python27-libs	2.7,18	
python27-lockfile	0.8	
python27-markupsafe	0,11	
python27-paramiko	1.15.1	
python27-pip	9.0.3	
python27-ply	3.4	
python27-pyasn1	0,17	
python27-pycurl	7,19,0	
python27-pygpgme	0.3	
python27-pyliblzma	0,5.3	
python27-pystache	0,5.3	
python27-pyxattr	0,5,0	
python27-requests	1.2.3	
python27-rsa	3.4.1	
python27-setuptools	36,2,7	

Package	AL1 AMI	AL2 AMI
python27-simplejson	3.6.5	
python27-six	1.8.0	
python27-urlgrabber	3,10	
python27-urllib3	1,24,3	
python27-virtualenv	15,10	
python3		3.7,16
python3-daemon		2.2.3
python3-docutils		0,14
python3-libs		3.7,16
python3-lockfile		0.11.0
python3-pip		20.2.2
python3-pystache		0,5.4
python3-setuptools		49,13
python3-simplejson		3.2.0
pyxattr		0,5.1
qrencode-libs		3.4.1
quota	4,00	4,01
quota-nls	4,00	4,01
rdate		1.4
readline	6.2	6.2

Package	AL1 AMI	AL2 AMI
rmt	0.4	
rng-tools	5	6.8
rootfiles	8.1	8.1
rpcbind	0.2.0	0.2.0
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-plugin-systemd-inhibit		4.11.3
rpm-python27	4.11.3	
rsync	3,0.6	3.1.2
rsyslog	5,8,10	8,24,0
ruby	2.0	
ruby20	2,0.0.648	
ruby20-irb	2,0.0.648	
ruby20-libs	2,0.0.648	
rubygem20-bigdecimal	1.2.0	
rubygem20-json	1.8.3	
rubygem20-psych	2.0.0	
rubygem20-rdoc	4.2.2	
rubygems20	2.0.14.1	

Package	AL1 AMI	AL2 AMI
scl-utils		20130529
screen	4.0.3	4.1.0
sed	4.2.1	4.2.2
selinux-policy		3.13.1
selinux-policy-targeted		3.13.1
sendmail	8,1,4	
setserial	2,17	2,17
configuration	2.8,14	2,8,71
setuptool		1,19,11
sgpio	1.2.0.10	1.2.0.10
shadow-utils	4.1.4.2	4.1.5.1
shared-mime-info	1.1	1.8
slang	2.2.1	2.2.4
sqlite	3.7,17	3.7,17
sssd-client		1,1,5
strace		4,26
sudo	1,8,23	1,8,23
sysctl-defaults	1.0	1.0
sysfsutils	2.1.0	
sysstat		10.1.5

Package	AL1 AMI	AL2 AMI
system-release	2018,03	2
systemd		219
systemd-libs		219
systemd-sysv		219
systemtap-runtime		4,5
sysvinit	2,87	
sysvinit-tools		2,88
tar	1,26	1,26
tcp_wrappers	7.6	7.6
tcp_wrappers-libs	7.6	7.6
tcpdump		4.9.2
tcsh		6,18,01
teamd		1,27
time	1.7	1,7
tmpwatch	2.9,16	
traceroute	2,0,14	2,0,22
ttmkfdir	3.0.9	
tzdata	2023c	2023c
tzdata-java	2023c	
udev	173	

Package	AL1 AMI	AL2 AMI
unzip	6.0	6.0
update-motd	1.0.1	1.1.2
upstart	0,6,5	
usermode		1,111
ustr	1.0.4	1.0.4
util-linux	2.23.2	2,30,2
vim-common	9,0.1712	9,0,2081
vim-data	9,0.1712	9,0,2081
vim-enhanced	9,0.1712	9,0,2081
vim-filesystem	9,0.1712	9,0,2081
vim-minimal	9,0.1712	9,0,2081
virt-what		1,18
wget	1,18	1.14
which	2,19	2,20
words	3.0	3.0
xfsdump		3.1.8
xfsprogs		5.0.0
xorg-x11-font-utils	7.2	
xorg-x11-fonts-Type1	7.2	
xxd	9,0.1712	9,0,2081

Package	AL1 AMI	AL2 AMI
xz	5.2.2	5.2.2
xz-libs	5.2.2	5.2.2
yajl		2.0.4
yum	3.4.3	3.4.3
yum-langpacks		0,4.2
yum-metadata-parser	1.1.4	1.1.4
yum-plugin-priorities	1.1.31	1.1.31
yum-plugin-upgrade-helper	1.1.31	
yum-utils	1.1.31	1.1.31
zip	3.0	3.0
zlib	1.2.8	1.2.7

Comparaison des packages installés sur les images du conteneur AL2 de base AL1 et des images

Package	AL1 Récipient	AL2 Récipient
amazon-linux-extras		2.0.3
basesystem	10,0	10,0
bash	4,2,46	4,2,46
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023,2,62	2023,2,62

Package	AL1 Récipient	AL2 Récipient
chkconfig	1.3.49.3	1.7.4
coreutils	8,22	8,22
cpio		2,12
curl	7,61,1	8.3.0
cyrus-sasl-lib	2.1.23	2.1.26
db4	4,7,25	
db4-utils	4,7,25	
diffutils		3.3
elfutils-libelf	0,168	0,176
expat	2.1.0	2.1.0
file-libs	5,37	5,11
filesystem	2,4,30	3.2
findutils		4.5.11
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
glib2	2,36.3	2,56.1
glibc	2,17	2,26
glibc-common	2,17	2,26
glibc-langpack-en		2,26
glibc-minimal-langpack		2,26

Package	AL1 Récipient	AL2 Récipient
gmp	6.0.0	6.0.0
gnupg2	2,0,28	2,0,22
gpgme	1.4.3	1.3.2
grep	2,20	2,20
gzip	1.5	
info	5.1	5.1
keyutils-libs	1.5.8	1.5.8
krb5-libs	1.15.1	1.15.1
libacl	2,2,49	2,2,51
libassuan	2.0.3	2.1.0
libattr	2,4,46	2,4,46
libblkid		2,30,2
libcap	2,16	2,54
libcom_err	1,43,5	1,42,9
libcrypt		2,26
libcurl	7,61,1	8.3.0
libdb		5.3.21
libdb-utils		5.3.21
libffi	3,0,13	3,0,13
libgcc		7.3.1

Package	AL1 Récipient	AL2 Récipient
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgpg-error	1.11	1.12
libicu	50,2	
libidn2	2.3.0	2.3.0
libmetalink		0,13
libmount		2,30,2
libnghttp2	1,33,0	1,41,0
libpsl	0.6.2	
libselinux	2.1.10	2,5
libsepol	2.1.7	2,5
libssh2	1.4.2	1.4.3
libstdc++		7.3.1
libstdc++72	7.2.1	
libtasn1	2.3	4,10
libunistring	0.9.3	0.9.3
libuuid		2,30,2
libverto	0,2,5	0,2,5
libxml2	2.9.1	2.9.1
libxml2-python27	2.9.1	

Package	AL1 Récipient	AL2 Récipient
lua	5.1.4	5.1.4
make	3,82	
ncurses	5.7	6.0
ncurses-base	5.7	6.0
ncurses-libs	5.7	6.0
nspr	4,25,0	4,35,0
nss	3,53,1	3,90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3,53,1	3,90,0
nss-softokn-freebl	3,53,1	3,90,0
nss-sysinit	3,53,1	3,90,0
nss-tools	3,53,1	3,90,0
nss-util	3,53,1	3,90,0
openldap	2,4,40	2,4,44
openssl	1,02k	
openssl-libs		1,02k
p11-kit	0,18,5	0,23,22
p11-kit-trust	0,18,5	0,23,22
pcre	8,21	8,32
pinentry	0,7,6	0.8.1

Package	AL1 Récipient	AL2 Récipient
pkgconfig	0,27,1	
popt	1.13	1.13
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0,5.3
python		2.7,18
python-iniparse		0.4
python-libs		2.7,18
python-pycurl		7,19,0
python-urlgrabber		3,10
python2-rpm		4.11.3
python27	2.7,18	
python27-chardet	2.0.1	
python27-iniparse	0,3.1	
python27-kitchen	1.1.1	
python27-libs	2.7,18	
python27-pycurl	7,19,0	
python27-pygpgme	0.3	
python27-pyliblzma	0,5.3	
python27-pyxattr	0,5,0	

Package	AL1 Récipient	AL2 Récipient
python27-urlgrabber	3,10	
pyxattr		0,5.1
readline	6.2	6.2
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-python27	4.11.3	
sed	4.2.1	4.2.2
configuration	2.8,14	2,8,71
shared-mime-info	1.1	1.8
sqlite	3.7,17	3.7,17
sysctl-defaults	1.0	
system-release	2018,03	2
tar	1,26	
tzdata	2023c	2023c
vim-data		9,0,2081
vim-minimal		9,0,2081
xz-libs	5.2.2	5.2.2
yum	3.4.3	3.4.3
yum-metadata-parser	1.1.4	1.1.4

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

AL2 sur Amazon EC2

> **Note**
>
> AL2 n'est plus la version actuelle d'Amazon Linux. AL2023 est le successeur de. AL2 Pour plus d'informations, consultez Comparing AL2 and AL2 023 et la liste des modifications de Package apportées à AL2 023 dans le Guide de l'utilisateur AL2023.

Rubriques

Lancer une EC2 instance Amazon avec AL2 AMI

Vous pouvez lancer une EC2 instance Amazon avec l' AL2 AMI. Pour plus d'informations, consultez Étape 1 : Lancer une instance.

Trouvez l' AL2 AMI la plus récente à l'aide de Systems Manager

Amazon EC2 fournit des paramètres AWS Systems Manager publics AMIs gérés par le public AWS que vous pouvez utiliser lors du lancement d'instances. Par exemple, le paramètre EC2 -provided `/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-default-hvm-x86_64-gp2`

est disponible dans toutes les régions et pointe toujours vers la dernière version de l' AL2 AMI dans une région donnée.

Pour trouver l'AMI AL2 023 la plus récente en utilisant AWS Systems Manager, voir Commencer avec AL2 023.

Les paramètres publics d'Amazon EC2 AMI sont disponibles via le chemin suivant :

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

Vous pouvez consulter la liste de tous les Amazon Linux AMIs de la AWS région actuelle en exécutant la AWS CLI commande suivante.

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

Pour lancer une instance à l'aide d'un paramètre public

L'exemple suivant utilise le paramètre public EC2 -provided pour lancer une `m5.xlarge` instance à l'aide de la dernière AL2 AMI.

Pour spécifier le paramètre dans la commande, utilisez la syntaxe suivante : `resolve:ssm:`*`public-parameter`*, où `resolve:ssm` est le préfixe standard et `public-parameter` le chemin et le nom du paramètre public.

Dans l'exemple, les paramètres `--count` et `--security-group` ne sont pas inclus. Pour `--count`, la valeur par défaut est 1. Si vous avez un VPC par défaut et un groupe de sécurité par défaut, ils sont utilisés.

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

Pour plus d'informations, consultez la section Utilisation de paramètres publics dans le Guide de AWS Systems Manager l'utilisateur.

Comprendre les noms des AMI Amazon Linux 2

Les noms des AMI Amazon Linux 2 utilisent le schéma de dénomination suivant :

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

- Minimal AMIs est fourni avec un ensemble réduit de packages préinstallés pour réduire la taille de l'image.
- La version du noyau détermine la version du noyau qui est préinstallée sur l'AMI correspondante :
  - `kernel-5.10`sélectionne la version 5.10 du noyau Linux. Il s'agit de la version de noyau recommandée pour AL2.
  - `kernel-default`sélectionne le noyau par défaut recommandé pour AL2. Il s'agit d'un alias pour kernel-5.10.
  - `kernel-4.14`sélectionne la version 4.14 du noyau Linux. Ceci n'est fourni que pour des raisons de compatibilité avec les anciennes versions de l'AMI. N'utilisez pas cette version pour le lancement de nouvelles instances. Attendez-vous à ce que cette AMI ne soit plus prise en charge.
  - Il existe un ensemble spécial de noms d'AMI sans référence à un noyau spécifique. Il s' AMIs agit d'un alias pour kernel-4.14. Ils ne AMIs sont fournis que pour des raisons de compatibilité avec les anciennes versions de l'AMI. N'utilisez pas ce nom d'AMI pour le lancement de nouvelles instances. Attendez-vous à ce que le noyau AMIs les mette à jour.
- x86_64/aarch64 détermine la plate-forme de processeur sur laquelle exécuter l'AMI. Sélectionnez x86_64 pour les instances basées sur Intel et AMD. EC2 Sélectionnez aarch64 pour les instances de EC2 Graviton.
- ebs/gp2 détermine le type de volume EBS utilisé pour servir l'AMI correspondante. Voir Types de volumes EBS pour référence. Sélectionnez toujours gp2.

Connect à une EC2 instance Amazon

Il existe plusieurs manières de se connecter à votre instance Amazon Linux, notamment SSH et EC2 Instance Connect. AWS Systems Manager Session Manager Pour plus d'informations, consultez Connect to your Linux instance dans le guide de EC2 l'utilisateur Amazon.

Les utilisateurs de SSH et sudo

Amazon Linux n'autorise pas le shell `root` sécurisé à distance (SSH) par défaut. L'authentification par mot de passe est également désactivée pour empêcher les attaques par force brute. Pour activer les connexions SSH à une instance Amazon Linux, vous devez fournir votre paire de clés à l'instance lors du lancement. Vous devez aussi définir le groupe de sécurité utilisé pour lancer votre

instance afin d'autoriser l'accès SSH. Par défaut, le seul compte qui peut se connecter à distance via SSH est `ec2-user`. Ce compte possède également sudo des privilèges. Si vous activez la `root` connexion à distance, sachez qu'elle est moins sûre que de vous fier à des paires de clés et à un utilisateur secondaire.

AL2 Mode de démarrage AMI

AL2 AMIs aucun paramètre de mode de démarrage n'est défini. Les instances lancées à partir de AL2 AMIs suivent la valeur du mode de démarrage par défaut du type d'instance. Pour plus d'informations, consultez la section Modes de démarrage dans le guide de EC2 l'utilisateur Amazon.

Référentiel de packages

Ces informations s'appliquent à AL2. Pour plus d'informations sur la AL2 version 023, consultez la section Gérer les packages et les mises à jour du système d'exploitation dans la AL2 version 023 du guide de l'utilisateur Amazon Linux 2023.

AL2 et AL1 sont conçus pour être utilisés avec les référentiels de packages en ligne hébergés dans chaque EC2 AWS région Amazon. Les référentiels sont disponibles dans toutes les régions et sont accessibles à l'aide des outils de mise à jour yum. L'hébergement de référentiels dans chaque région nous permet de déployer rapidement les mises à jour et sans aucuns frais de transfert de données.

> **Important**
>
> La dernière version de AL1 EOL a pris fin le 31 décembre 2023 et ne recevra aucune mise à jour de sécurité ni aucune correction de bogue à compter du 1er janvier 2024. Pour plus d'informations, consultez AMI Amazon Linux end-of-life.

Si vous n'avez pas besoin de conserver les données ou de personnaliser vos instances, vous pouvez lancer de nouvelles instances à l'aide de l' AL2 AMI actuelle. Si vous devez conserver les données ou les personnalisations de vos instances, vous pouvez gérer ces instances via les référentiels de packages Amazon Linux. Ces référentiels contiennent tous les packages mis à jour. Vous pouvez choisir d'appliquer ces mises à jour à vos instances en cours d'exécution. Les versions antérieures de l'AMI et les packages de mise à jour restent disponibles, même lorsque de nouvelles versions sont publiées.

> **Note**
>
> Pour mettre à jour et installer des packages sans accès à Internet sur une EC2 instance Amazon, consultez Comment puis-je mettre à jour yum ou installer des packages sans accès à Internet sur mes EC2 instances Amazon en cours d'exécution AL1 AL2, ou AL2 023 ?

Pour installer des packages, utilisez la commande suivante :

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

Si vous découvrez qu'Amazon Linux ne contient pas une application dont vous avez besoin, vous pouvez installer l'application directement sur votre instance Amazon Linux. Amazon Linux utilise RPMs et yum pour la gestion des packages, et c'est probablement le moyen le plus direct d'installer de nouvelles applications. Vous devriez vérifier si une application est déjà disponible dans notre référentiel central d'Amazon Linux, car beaucoup d'applications sont disponibles ici. À partir de là, vous pouvez ajouter ces applications à votre instance Amazon Linux.

Pour charger vos applications sur une instance Amazon Linux en cours d'exécution, utilisez scp ou sftp, puis configurez l'application en vous connectant à votre instance. Vos applications peuvent aussi être chargées pendant le lancement de l'instance en utilisant l'action PACKAGE_SETUP à partir du package cloud-init intégré. Pour plus d'informations, consultez Utilisation de cloud-init sur AL2.

Mises à jour de sécurité

Les mises à jour de sécurité sont fournies à l'aide des référentiels de packages. Les mises à jour de sécurité et les alertes de sécurité AMI mises à jour sont publiées dans le centre de sécurité Amazon Linux. Pour plus d'informations sur les politiques de sécurité AWS ou pour signaler un problème de sécurité, consultez Sécurité du cloud AWS.

AL1 et AL2 sont configurés pour télécharger et installer des mises à jour de sécurité critiques ou importantes au moment du lancement. Les mises à jour du noyau ne sont pas incluses dans cette configuration.

En AL2 023, cette configuration a changé par rapport à AL1 et AL2. Pour plus d'informations sur les mises à jour de sécurité pour AL2 023, consultez la section Mises à jour et fonctionnalités de sécurité dans le guide de l'utilisateur Amazon Linux 2023.

Nous vous recommandons d'effectuer les mises à jour nécessaires pour votre cas d'utilisation après le lancement. Par exemple, vous souhaiterez peut-être appliquer toutes les mises à jour (pas uniquement les mises à jour de sécurité) au lancement, ou évaluer chaque mise à jour et appliquer uniquement celles applicables à votre système. Ceci est contrôlé à l'aide du paramètre cloud-init suivant : `repo_upgrade`. L'extrait de configuration cloud-init suivant montre comment modifier les paramètres dans le texte de données utilisateur que vous transmettez à l'initialisation de votre instance :

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

Les valeurs possibles pour `repo_upgrade` sont les suivantes :

`critical`

Appliquez les mises à jour de sécurité critiques en attente.

`important`

Appliquez les mises à jour de sécurité importantes et critiques.

`medium`

Appliquez les mises à jour de sécurité critiques, importantes et moyennes.

`low`

Appliquez toutes les mises à jour de sécurité en attente, y compris les mises à jour de sécurité de faible gravité.

`security`

Appliquez les mises à jour critiques ou importantes indiquées par Amazon comme étant des mises à jour de sécurité.

`bugfix`

Appliquez les mises à jour indiquées par Amazon comme étant des correctifs de bogues. Les correctifs de bogues constituent un ensemble plus important de mises à jour ce qui comprend des mises à jour de sécurité et des correctifs pour plusieurs autres bogues mineurs.

`all`

Appliquez toutes les mises à jour disponibles appropriées, peu importe leur classification.

`none`

N'appliquez aucune mise à jour à l'instance au démarrage.

> **Remarque**
>
> Amazon Linux ne marque aucune mise à jour comme`bugfix`. Pour appliquer des mises à jour non liées à la sécurité depuis Amazon Linux, utilisez`repo_upgrade: all`.

Le paramètre par défaut pour `repo_upgrade` est la sécurité. En effet, si vous ne spécifiez pas une valeur différente dans vos données utilisateur, Amazon Linux effectue par défaut les mises à niveau de sécurité au lancement pour tous les packages installés à ce moment. Amazon Linux vous informe également de toute mise à jour des packages installés en listant le nombre de mises à jour disponibles lors de la connexion à l'aide de `/etc/motd` dans le fichier. Pour installer ces mises à jour, vous devez exécuter sudo yum upgrade sur l'instance.

Configuration du référentiel

Pour AL1 et AL2, AMIs sont un instantané des packages disponibles au moment de la création de l'AMI, à l'exception des mises à jour de sécurité. Tous les packages ne figurant pas sur l'AMI d'origine, mais installés au moment de l'exécution, seront les dernières versions disponibles. Pour obtenir les derniers packages disponibles pour AL2, exécutez`yum update -y`.

> **Conseil pour la résolution de problèmes**
>
> Si vous recevez une `cannot allocate memory` erreur lors de l'exécution yum update sur les types d'instances nano, par exemple`t3.nano`, vous devrez peut-être allouer de l'espace d'échange pour activer la mise à jour.

Pour AL2 023, la configuration du référentiel a changé par rapport à AL1 et AL2. Pour plus d'informations sur le référentiel AL2 023, consultez la section Gestion des packages et des mises à jour du système d'exploitation.

Les versions antérieures à AL2 023 ont été configurées pour fournir un flux continu de mises à jour permettant de passer d'une version mineure d'Amazon Linux à la version suivante, également

appelée versions continues. Il est recommandé de mettre à jour votre AMI avec la dernière AMI disponible plutôt que de lancer les anciennes AMIs et d'appliquer des mises à jour.

Les mises à niveau sur place ne sont pas prises en charge entre les principales versions d'Amazon Linux, par AL1 exemple entre et AL2 AL2 023. AL2 Pour de plus amples informations, veuillez consulter Disponibilité Amazon Linux.

Utilisation de cloud-init sur AL2

Le package cloud-init est une application open source créée par Canonical qui est utilisée pour démarrer des images Linux dans un environnement de cloud computing, tel qu'Amazon. EC2 Amazon Linux contient une version personnalisée de cloud-init. Cela vous permet de spécifier les actions qui doivent être exécutées sur votre instance au moment du démarrage. Vous pouvez transmettre les actions souhaitées à cloud-init via les champs de données utilisateur lors du lancement d'une instance. Cela signifie que vous pouvez utiliser Common AMIs pour de nombreux cas d'utilisation et les configurer dynamiquement au démarrage. Amazon Linux utilise aussi cloud-init pour effectuer une configuration initiale du compte utilisateur ec2-user.

Pour plus d'informations, consultez la documentation cloud-init.

Amazon Linux utilise les actions cloud-init trouvées dans `/etc/cloud/cloud.cfg.d` et `/etc/cloud/cloud.cfg`. Vous pouvez créer vos propres fichiers d'actions cloud-init dans `/etc/cloud/cloud.cfg.d`. Tous les fichiers dans ce répertoire sont lus par cloud-init. Ils sont lus en ordre lexical, et les fichiers plus récents remplacent les valeurs des fichiers plus anciens.

Le package cloud-init effectue des tâches de configuration communes (et d'autres tâches) pour les instances au démarrage :

- Définir les paramètres régionaux par défaut.
- Définir le nom d'hôte.
- Analyser et gérer les données utilisateur.
- Générer des clés SSH privées d'hôte.
- Ajouter des clés SSH publiques d'utilisateur à `.ssh/authorized_keys` pour une connexion et une administration faciles.
- Préparer les référentiels pour la gestion des packages.
- Gérer les actions de package définies dans les données utilisateur.
- Exécutez les scripts utilisateur trouvés dans les données utilisateur.

- Monter les volumes de stockage d'instance, le cas échéant.
  - Par défaut, le volume de stockage d'instance `ephemeral0` est monté sur `/media/ephemeral0` s'il est présent et contient un système de fichiers valide ; sinon, il n'est pas monté.
  - Par défaut, les volumes d'échange associés à l'instance sont montés (uniquement pour les types d'instance `m1.small` et `c1.medium`).
  - Vous pouvez remplacer le montage de volume de stockage d'instance par défaut avec la directive cloud-init suivante :

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

    Pour plus de contrôle sur les montages, consultez Mounts dans la documentation cloud-init.
  - Les volumes de stockage d'instance qui prennent en charge la commande TRIM ne sont pas formatés au lancement de l'instance. Vous devez donc les partitionner et les formater pour pouvoir les monter et les utiliser. Pour plus d'informations, consultez la section Prise en TRIMcharge du volume de stockage d'instance. Vous pouvez utiliser le module `disk_setup` pour partitionner et formater vos volumes de stockage d'instance au démarrage. Pour plus d'informations, consultez Disk Setup dans la documentation cloud-init.

Formats de données utilisateur pris en charge

Le package cloud-init prend en charge le traitement des données utilisateur sous différents formats :

- Gzip
  - Si les données utilisateur sont compressées au format gzip, cloud-init les décompresse et les gère de manière appropriée.
- Fichier MIME en plusieurs parties
  - En utilisant un fichier MIME en plusieurs parties, vous pouvez spécifier plus d'un type de données. Par exemple, vous pouvez spécifier à la fois un script de données utilisateur et un type de configuration cloud. Chaque partie de ce fichier peut être traitée par cloud-init s'il s'agit d'un des formats pris en charge.
- Décodage Base64

  - Si les données utilisateur sont codées en base64, cloud-init détermine s'il peut comprendre les données décodées comme l'un des types pris en charge. S'il comprend les données décodées, il décode les données et les gère de façon appropriée. Si non, il renvoie les données base64 intactes.
- Script de données utilisateur
  - Commence par `#!` ou `Content-Type: text/x-shellscript`.
  - Le script est exécuté par `/etc/init.d/cloud-init-user-scripts` pendant le premier cycle de démarrage. Cela se produit tard dans le processus de démarrage (après l'exécution des actions de configuration initiales).
- Fichier d'inclusion
  - Commence par `#include` ou `Content-Type: text/x-include-url`.
  - Ce contenu est un fichier d'inclusion. Le fichier contient une liste de URLs, une par ligne. Chacun d'entre eux URLs est lu et leur contenu est soumis à ce même ensemble de règles. Le contenu lu à partir de l'URL peut être compressé au format gzip ou MIME-multi-part en texte brut.
- Données de configuration du cloud
  - Commence par `#cloud-config` ou `Content-Type: text/cloud-config`.
  - Ce contenu est constitué de données de configuration du cloud.
- Tâche initiale (non prise en charge sur AL2)
  - Commence par `#upstart-job` ou `Content-Type: text/upstart-job`.
  - Ce contenu est stocké dans un fichier dans`/etc/init`, et upstart consomme le contenu comme c'est le cas pour les autres tâches de démarrage.
- Crochet en forme de cloud
  - Commence par `#cloud-boothook` ou `Content-Type: text/cloud-boothook`.
  - Ce contenu correspond aux données boothook. Il est stocké dans un fichier sous `/var/lib/cloud`, puis exécuté immédiatement.
  - Il s'agit du hook le plus récent disponible. Il n'existe aucun mécanisme proposé pour l'exécuter seulement une fois. Le boothook doit s'en occuper lui-même. Il est fourni avec l'ID d'instance dans la variable d'environnement `INSTANCE_ID`. Utilisez cette variable pour fournir un once-per-instance ensemble de données de démarrage.

Configuration AL2 des instances

Une fois que vous avez lancé et connecté votre AL2 instance avec succès, vous pouvez y apporter des modifications. Il existe de nombreuses façons différentes de configurer une instance afin de répondre aux besoins d'une application spécifique. Les tâches suivantes comptent parmi celles couramment utilisées pour vous permettre de débuter.

Sommaire

Scénarios de configuration courants

La distribution de base d'Amazon Linux contient les packages logiciels et les utilitaires nécessaires aux opérations de base du serveur. Néanmoins, beaucoup plus de packages logiciels sont disponibles dans différents référentiels de logiciels et encore plus de packages sont disponibles pour permettre la création à partir du code source. Pour plus d'informations sur l'installation et la création de logiciels à partir de ces emplacements, consultez le didacticiel Gérez les logiciels sur votre AL2 instance.

Les instances Amazon Linux sont préconfigurées avec un `ec2-user`, mais il se peut que vous souhaitiez ajouter d'autres utilisateurs qui n'ont pas de privilèges du super-utilisateur. Pour plus d'informations sur l'ajout et la suppression d'utilisateurs, consultez Gérer les utilisateurs sur votre Linux instance dans le guide de EC2 l'utilisateur Amazon.

Si vous possédez votre propre réseau avec un nom de domaine enregistré, vous pouvez changer le nom d'hôte d'une instance pour l'identifier dans le cadre de ce domaine. Vous pouvez aussi changer l'invite du système pour avoir un nom plus descriptif sans changer les réglages du nom d'hôte. Pour plus d'informations, consultez Modifier le nom d'hôte de votre instance AL2 . Vous pouvez configurer une instance pour utiliser un fournisseur de services DNS dynamiques. Pour de plus amples informations, veuillez consulter Configurer le DNS dynamique sur votre AL2 instance.

Lorsque vous lancez une instance sur Amazon EC2, vous avez la possibilité de lui transmettre des données utilisateur qui peuvent être utilisées pour effectuer des tâches de configuration courantes et même exécuter des scripts après le démarrage de l'instance. Vous pouvez transmettre deux types de données utilisateur à Amazon EC2 : les directives cloud-init et les scripts shell. Pour plus d'informations, consultez la section Exécuter des commandes sur votre Linux instance au lancement dans le guide de EC2 l'utilisateur Amazon.

Gérez les logiciels sur votre AL2 instance

La distribution de base d'Amazon Linux contient les packages logiciels et les utilitaires nécessaires aux opérations de base du serveur.

Ces informations s'appliquent à AL2. Pour plus d'informations sur la AL2 version 023, consultez la section Gérer les packages et les mises à jour du système d'exploitation dans la AL2 version 023 du guide de l'utilisateur Amazon Linux 2023.

Il est important de garder les logiciels à jour. Beaucoup de packages dans une distribution Linux sont souvent mis à jour pour résoudre les bogues, ajouter des fonctions et protéger contre le code malveillant. Pour de plus amples informations, veuillez consulter Mettre à jour le logiciel de l'instance sur votre AL2 instance.

Par défaut, AL2 les instances sont lancées avec les référentiels suivants activés :

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

Bien que de nombreux packages soient disponibles dans ces référentiels et mis à jour par AWS, il se peut que vous souhaitiez installer un package contenu dans un autre référentiel. Pour de plus amples informations, veuillez consulter Ajouter des référentiels sur une instance AL2 . Pour obtenir de l'aide pour trouver et installer des packages dans les référentiels activés, consultez Rechercher et installer des packages logiciels sur une AL2 instance.

Les logiciels ne sont pas tous disponibles dans les packages logiciels stockés dans les référentiels. Certains logiciels doivent être compilés sur une instance à partir de son code source. Pour de plus amples informations, veuillez consulter Préparation à la compilation du logiciel sur une AL2 instance.

AL2 les instances gèrent leurs logiciels à l'aide du gestionnaire de packages yum. Le gestionnaire de packages yum peut installer, supprimer et mettre à jour les logiciels ainsi que gérer l'ensemble des dépendances pour chaque package.

Table des matières

Mettre à jour le logiciel de l'instance sur votre AL2 instance

Il est important de garder les logiciels à jour. Les packages dans une distribution Linux sont souvent mis à jour pour résoudre les bogues, ajouter des fonctions et protéger contre le code malveillant. Lorsque vous lancez et vous vous connectez pour la première fois à une instance Amazon Linux, il se peut que vous voyez un message vous demandant de mettre à jour des packages logiciels à des fins de sécurité. Cette section explique comment mettre à jour l'ensemble d'un système ou juste un seul package.

Ces informations s'appliquent à AL2. Pour plus d'informations sur la AL2 version 023, consultez la section Gérer les packages et les mises à jour du système d'exploitation dans la AL2 version 023 du guide de l'utilisateur Amazon Linux 2023.

Pour plus d'informations sur les modifications et les mises à jour apportées à AL2, consultez les notes AL2 de publication.

Pour plus d'informations sur les modifications et les mises à jour apportées à la version AL2 023, consultez les notes de mise à jour de la version AL2 023.

> **Important**
>
> Si vous avez lancé une EC2 instance qui utilise une AMI Amazon Linux 2 dans un sous-réseau IPv6 réservé, vous devez vous connecter à l'instance et l'exécuter. `sudo amazon-linux-https disable` Cela permet à votre AL2 instance de se connecter au yum référentiel dans S3 IPv6 via le service de correctif HTTP.

Pour mettre à jour tous les packages d'une AL2 instance

1. (Facultatif) Lancez une session screen dans votre fenêtre shell. Il se peut que vous connaissiez parfois une interruption du réseau qui peut déconnecter la connexion SSH à votre instance. Si ce problème arrive pendant une longue mise à jour logicielle, cela peut laisser l'instance dans un

état récupérable bien que désorienté. Une session screen vous permet de continuer à exécuter la mise à jour même si votre connexion est interrompue et vous pouvez vous reconnecter à la session plus tard sans problème.

a. Exécutez la commande screen pour démarrer la session.

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

b. Si votre session est déconnectée, reconnectez-vous à votre instance et énumérez les écrans disponibles.

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

c. Reconnectez-vous à l'écran à l'aide de la commande screen -r et l'ID du processus de la commande précédente.

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

d. Lorsque vous avez terminé d'utiliser screen, servez-vous de la commande exit pour fermer la session.

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

2. Exécutez la commande yum update. Le cas échéant, vous pouvez ajouter l'indicateur `--security` pour appliquer uniquement les mises à jour de sécurité.

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

3. Vérifiez les packages énumérés, saisissez **y**, puis appuyez sur Entrée pour accepter les mises à jour. La mise à jour de tous les packages d'un système peut prendre plusieurs minutes. Les résultats yum montrent le statut de la mise à jour pendant son exécution.
4. (Facultatif) Redémarrez votre instance pour vous assurer que vous utilisez les derniers packages et bibliothèques issus de votre mise à jour ; les mises à jour du noyau ne sont pas chargées tant qu'un redémarrage n'est pas effectué. Les mises à jour de n'importe quelle bibliothèque `glibc` devraient aussi être suivies d'un redémarrage. Pour les mises à jour des packages qui contrôlent les services, il peut s'avérer suffisant de redémarrer les services pour récupérer les mises à jour,

mais un redémarrage du système assure que toutes les mises à jour précédentes des packages et des bibliothèques sont terminées.

Pour mettre à jour un seul package sur une AL2 instance

Utilisez cette procédure pour mettre à jour un seul package (et ses dépendances) et non l'ensemble du système.

1. Exécutez la commande yum update avec le nom du package que vous souhaiteriez mettre à jour.

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

2. Vérifiez les détails relatifs aux packages énumérés, saisissez **y**, puis appuyez sur Entrée pour accepter les mises à jour. Il peut arriver qu'il y ait plus d'un package énuméré s'il existe des dépendances de packages qui doivent être résolues. Les résultats yum montrent le statut de la mise à jour pendant son exécution.
3. (Facultatif) Redémarrez votre instance pour vous assurer que vous utilisez les derniers packages et bibliothèques issus de votre mise à jour ; les mises à jour du noyau ne sont pas chargées tant qu'un redémarrage n'est pas effectué. Les mises à jour de n'importe quelle bibliothèque `glibc` devraient aussi être suivies d'un redémarrage. Pour les mises à jour des packages qui contrôlent les services, il peut s'avérer suffisant de redémarrer les services pour récupérer les mises à jour, mais un redémarrage du système assure que toutes les mises à jour précédentes des packages et des bibliothèques sont terminées.

Ajouter des référentiels sur une instance AL2

Ces informations s'appliquent à AL2. Pour plus d'informations sur le AL2 023, consultez la section Mises à niveau déterministes via des référentiels versionnés sur 023 AL2 dans le guide de l'utilisateur Amazon Linux 2023.

Par défaut, AL2 les instances sont lancées avec les référentiels suivants activés :

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

S'il existe de nombreux packages disponibles dans ces référentiels qui sont mis à jour par Amazon Web Services, il est toutefois possible que vous trouviez un package dans un autre référentiel que vous souhaitez installer.

Pour installer un package d'un référentiel différent avec la commande yum, vous devez ajouter les détails relatifs au référentiel au fichier `/etc/yum.conf` ou à son propre fichier *`repository`*`.repo` dans le répertoire `/etc/yum.repos.d`. Vous pouvez le faire manuellement, mais la plupart des référentiels yum ont leur propre fichier *`repository`*`.repo` sur l'URL de leur référentiel.

Pour déterminer quels référentiels yum sont déjà installés

Utilisez la commande suivante pour répertorier les référentiels yum installés :

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

La sortie obtenue répertorie les référentiels installés et indique l'état de chacun. Les référentiels activés affichent le nombre de packages qu'ils contiennent.

Pour ajouter un référentiel yum à /etc/yum.repos.d

1. Recherchez l'emplacement du fichier `.repo`. Il variera selon le référentiel que vous ajoutez. Dans cet exemple, le fichier `.repo` se trouve à l'adresse `https://www.`*`example`*`.com/`*`repository`*`.repo`.
2. Ajoutez le référentiel à l'aide de la commande yum-config-manager.

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

Après avoir installé un référentiel, vous devez l'activer, comme décrit dans la procédure suivante.

Pour activer un référentiel yum dans /etc/yum.repos.d

Utilisez la commande yum-config-manager avec l'indicateur `--enable` *`repository`*. La commande suivante active le référentiel EPEL (Extra Packages for Enterprise Linux) à partir du projet Fedora.

Par défaut, ce référentiel est présent dans `/etc/yum.repos.d` sur les instances Amazon Linux AMI, mais il n'est pas activé.

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

Pour plus d'informations et pour télécharger la dernière version de ce package, consultez https:// fedoraproject. org/wiki/EPEL.

Rechercher et installer des packages logiciels sur une AL2 instance

Vous pouvez utiliser un outil de gestion des packages pour trouver et installer des packages logiciels. Dans Amazon Linux 2, l'outil de gestion des packages logiciels par défaut estYUM. Dans AL2 023, l'outil de gestion des progiciels par défaut estDNF. Pour plus d'informations, consultez l'outil de gestion des packages dans le guide de l'utilisateur Amazon Linux 2023.

Rechercher des packages logiciels sur une AL2 instance

Vous pouvez utiliser la commande yum search pour rechercher les descriptions des packages qui sont disponibles dans vos référentiels configurés. Elle est particulièrement utile si vous ne connaissez pas le nom exact du package que vous voulez installer. Il suffit de joindre la recherche de mots clés à la commande ; pour les recherches de plusieurs mots, entourez la requête de recherche avec des guillemets.

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

Voici un exemple de sortie.

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
============================== N/S matched: find ===============================
findutils.x86_64 : The GNU versions of find utilities (find and xargs)
gedit-plugin-findinfiles.x86_64 : gedit findinfiles plugin
ocaml-findlib-devel.x86_64 : Development files for ocaml-findlib
perl-File-Find-Rule.noarch : Perl module implementing an alternative interface to
 File::Find
robotfindskitten.x86_64 : A game/zen simulation. You are robot. Your job is to find
 kitten.
mlocate.x86_64 : An utility for finding files by name
ocaml-findlib.x86_64 : Objective CAML package manager and build helper
perl-Devel-Cycle.noarch : Find memory cycles in objects
perl-Devel-EnforceEncapsulation.noarch : Find access violations to blessed objects
perl-File-Find-Rule-Perl.noarch : Common rules for searching for Perl things
```

```
perl-File-HomeDir.noarch : Find your home and other directories on any platform
perl-IPC-Cmd.noarch : Finding and running system commands made easy
perl-Perl-MinimumVersion.noarch : Find a minimum required version of perl for Perl code
texlive-xesearch.noarch : A string finder for XeTeX
valgrind.x86_64 : Tool for finding memory management bugs in programs
valgrind.i686 : Tool for finding memory management bugs in programs
```

Les demandes de recherche de plusieurs mots entre guillemets donnent uniquement des résultats qui correspondent à la requête exacte. Si vous ne voyez pas le package attendu, simplifiez votre recherche en utilisant un mot clé, puis analyser les résultats. Vous pouvez aussi des synonymes des mots clés pour élargir votre recherche.

Pour plus d'informations sur les packages pour AL2, consultez les rubriques suivantes :

- AL2 Bibliothèque d'extras
- Référentiel de packages

Installation de packages logiciels sur une AL2 instance

Dans AL2, l'outil de gestion de packages yum recherche les différents packages logiciels dans tous vos référentiels activés et gère toutes les dépendances du processus d'installation du logiciel. Pour plus d'informations sur l'installation de packages logiciels dans la AL2 version 023, consultez la section Gestion des packages et des mises à jour du système d'exploitation dans le guide de l'utilisateur Amazon Linux 2023.

Pour installer un package à partir d'un référentiel

Utilisez la yum install ***package*** commande en *package* remplaçant par le nom du logiciel à installer. Par exemple, pour installer le navigateur web à base de texte links, saisissez la commande suivante.

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

Pour installer les fichiers du package RPM que vous avez téléchargé

Vous pouvez également utiliser yum install pour installer les fichiers du package RPM que vous avez téléchargé sur Internet. Pour cela, il vous suffit de joindre le nom du chemin d'un fichier RPM à la commande d'installation au lieu du nom d'un package de référentiel.

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

Pour lister les packages installés

Pour afficher la liste des packages installés sur votre instance, utilisez la commande suivante.

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

Préparation à la compilation du logiciel sur une AL2 instance

Les logiciels open source sont disponibles sur Internet qui n'ont pas été précompilés et mis à disposition pour le téléchargement à partir d'un référentiel de packages. Il est possible que vous découvriez un package logiciel que vous devrez compiler vous-même, à partir de son code source. Pour que votre système puisse compiler des logiciels dans AL2 Amazon Linux, vous devez installer plusieurs outils de développement, tels que makegcc, etautoconf.

La compilation de logiciels n'étant pas une tâche requise par toutes les EC2 instances Amazon, ces outils ne sont pas installés par défaut, mais ils sont disponibles dans un groupe de packages appelé « Outils de développement » qui peut être facilement ajouté à une instance à l'aide de la yum groupinstall commande.

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

Les packages de code source des logiciels sont souvent disponibles en téléchargement (à partir de sites Web tels que https://github.com/et http://sourceforge.net/) sous forme de fichier d'archive compressé, appelé tarball. Ces tarballs portent généralement l'extension de fichier `.tar.gz`. Vous pouvez décompresser ces archives avec la commande tar.

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

Après avoir décompressé et désarchivé le package de code source, vous devriez rechercher un fichier `README` ou `INSTALL` dans le répertoire du code source qui peut vous fournir plus d'instructions pour la compilation et l'installation du code source.

Pour récupérer le code source des packages Amazon Linux

Amazon Web Services fournit le code source pour les packages gérés. Vous pouvez télécharger le code source pour n'importe quel package installé avec la commande yumdownloader --source.

Exécutez la yumdownloader --source *package* commande pour télécharger le code source de*package*. Par exemple, pour télécharger le code source du package `htop`, saisissiez la commande suivante.

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

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

L'emplacement du fichier RPM source est dans le répertoire à partir duquel vous avez exécuté la commande.

Contrôle de l'état du processeur pour votre EC2 AL2 instance Amazon

Les états « C-states » contrôlent les niveaux de veille qu'un élément central peut atteindre lorsqu'il est inactif. Les états « C-state » sont numérotés de C0 (l'état le plus superficiel lorsque le cœur est totalement éveillé et exécute les instructions) à C6 (l'état de veille le plus profond lorsqu'un cœur est arrêté).

Les états « P-states » contrôlent les performances souhaitées (dans la fréquence de l'UC) à partir d'un cœur. La numérotation des états « P-states » commence à P0 (paramètre de performance le plus élevé dans lequel le cœur peut utiliser la technologie Intel Turbo Boost pour améliorer la fréquence si possible) et va de P1 (état « P-state » qui demande la fréquence de base maximale) à P15 (fréquence la plus basse possible).

Il se peut que vous vouliez changer les paramètres « C-state » ou « P-state » pour améliorer la cohérence des performances du processeur, réduire la latence ou ajuster votre instance pour une charge de travail spécifique. Les paramètres « C-state » ou « P-state » par défaut offre des performances maximales qui sont optimales pour la plupart des charges de travail. Cependant, si votre application tirerait avantage de la latence réduite pour un coût de fréquences simple ou double cœur plus hautes ou des performances cohérentes à des fréquences plus basses au lieu des fréquences Turbo Boost transmises en paquets, pensez à essayer les paramètres « C-state » ou « P-state » qui sont disponibles pour ces instances.

Pour plus d'informations sur les types d' EC2 instances Amazon qui permettent au système d'exploitation de contrôler les états C et P du processeur, consultez la section Contrôle de l'état du processeur pour votre EC2 instance Amazon dans le guide de EC2 l'utilisateur Amazon.

Les sections suivantes décrivent les différentes configurations d'états du processeur et les façons de surveiller les effets de votre configuration. Ces procédures ont été écrites pour Amazon Linux et s'appliquent à celui-ci ; toutefois, elles peuvent également fonctionner pour d'autres distributions Linux dotées d'une version de noyau Linux 3.9 ou ultérieure.

> **Note**
>
> Les exemples présentés sur cette page utilisent les éléments suivants :
>
> - L'utilitaire turbostat pour afficher les informations relatives à la fréquence du processeur et à l'état « C-state ». L'utilitaire turbostat est disponible sur Amazon Linux par défaut.
> - La commande stress pour simuler une charge de travail. Pour installer stress, commencez par activer le référentiel EPEL en exécutant sudo amazon-linux-extras install epel, puis exécutez sudo yum install -y stress.
>
> Si la sortie n'affiche pas les informations relatives à l'état « C-state », incluez l'option --debug dans la commande (sudo turbostat --debug stress ***<options>***).

Sommaire

La meilleure performance avec la fréquence Turbo Boost maximale

Il s'agit de la configuration de contrôle d'état du processeur par défaut pour Amazon Linux AMI et il est recommandé pour la plupart des charges de travail. Cette configuration fournit les meilleures performances avec des variations plus faibles. Le fait de permettre aux cœurs inactifs d'entrer dans des états de veille plus profonds offre le dégagement thermique nécessaire aux processeurs simple ou double cœur d'atteindre leur potentiel Turbo Boost maximal.

L'exemple suivant montre une instance `c4.8xlarge` avec deux cœurs qui fonctionnent activement et atteignent la fréquence Turbo Boost maximale de leur processeur.

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

Dans cet exemple, les versions CPUs 21 et 28 fonctionnent à leur fréquence Turbo Boost maximale parce que les autres cœurs sont entrés en état de C6 veille pour économiser de l'énergie et fournir à la fois de l'énergie et de la marge thermique aux cœurs de travail. Les versions CPUs 3 et 10 (chacune partageant un cœur de processeur avec les C1 v CPUs 21 et 28) sont en attente d'instructions.

Dans l'exemple suivant, les 18 cœurs travaillent activement. Il n'y a donc pas de marge de manœuvre pour un Turbo Boost maximal, mais ils fonctionnent tous à la vitesse « Turbo Boost tous les cœurs » de 3,2 GHz.

```
[ec2-user ~]$ sudo turbostat stress -c 36 -t 10
stress: info: [30685] dispatching hogs: 36 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30685] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
  Pkg_W RAM_W PKG_% RAM_%
           99.27 3.20 2.90   0   0.26   0.00   0.47   0.00   0.00   0.00   0.00   0.00
 228.59 31.33 199.26  0.00
```

```
 0   0   0  99.08 3.20 2.90   0   0.27   0.01   0.64   0.00   0.00   0.00   0.00   0.00
 114.69 18.55 99.32  0.00
 0   0  18  98.74 3.20 2.90   0   0.62
 0   1   1  99.14 3.20 2.90   0   0.09   0.00   0.76   0.00
 0   1  19  98.75 3.20 2.90   0   0.49
 0   2   2  99.07 3.20 2.90   0   0.10   0.02   0.81   0.00
 0   2  20  98.73 3.20 2.90   0   0.44
 0   3   3  99.02 3.20 2.90   0   0.24   0.00   0.74   0.00
 0   3  21  99.13 3.20 2.90   0   0.13
 0   4   4  99.26 3.20 2.90   0   0.09   0.00   0.65   0.00
 0   4  22  98.68 3.20 2.90   0   0.67
 0   5   5  99.19 3.20 2.90   0   0.08   0.00   0.73   0.00
 0   5  23  98.58 3.20 2.90   0   0.69
 0   6   6  99.01 3.20 2.90   0   0.11   0.00   0.89   0.00
 0   6  24  98.72 3.20 2.90   0   0.39
...
```

Haute performance et faible latence en limitant les états « C-state » plus profonds

Les états « C-state » contrôlent les niveaux de veille dans lesquels un cœur peut entrer lorsqu'il est inutilisé. Il se peut que vous vouliez contrôler les états « C-state » pour ajuster la latence de votre système par rapport aux performances. La mise en veille de cœurs prend du temps. Même si un cœur en veille donne plus de marge pour qu'un autre cœur fonctionne à une fréquence plus élevée, ce cœur en veille prend du temps pour se remettre en route et fonctionner. Par exemple, si un cœur qui est assigné à la gestion d'interruptions de paquets est en veille, il se peut que la prise en charge de cette interruption soit retardée. Vous pouvez configurer le système pour qu'il n'utilise pas les états « C-state » plus profonds ce qui réduit la latence de réaction du processeur, mais également la marge disponible pour la fréquence Turbo Boost des autres cœurs.

Un scénario commun pour la désactivation d'états de veille plus profonds est une application de la base de données Redis qui stocke la base de données dans la mémoire système pour un temps de réponse aux requêtes le plus rapide possible.

Pour limiter les états de sommeil plus profonds sur AL2

1. Ouvrez le fichier `/etc/default/grub` avec l'éditeur de votre choix.

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

2. Modifiez la ligne `GRUB_CMDLINE_LINUX_DEFAULT` et ajoutez l'option `intel_idle.max_cstate=1` pour `processor.max_cstate=1` définir `C1` comme l'état « C-state » le plus profond pour les cœurs inutilisés.

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

   L'option `intel_idle.max_cstate=1` configure la limite de l'état C pour les instances Intel, et l'option `processor.max_cstate=1` configure la limite de l'état C pour les instances basées sur AMD. Il est possible d'ajouter les deux options à votre configuration en toute sécurité. Cela permet à une configuration unique de définir le comportement souhaité sur Intel et AMD.

3. Enregistrez le fichier et quittez votre éditeur.

4. Exécutez la commande suivante pour recréer la configuration du démarrage.

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

5. Redémarrez votre instance pour activer la nouvelle option noyau.

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

Pour limiter les états de veille plus profonds sur Amazon Linux AMI

1. Ouvrez le fichier `/boot/grub/grub.conf` avec l'éditeur de votre choix.

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

2. Modifiez la ligne `kernel` de la première entrée et ajoutez les options `intel_idle.max_cstate=1` et `processor.max_cstate=1` pour définir `C1` comme l'état « C-state » le plus profond pour les cœurs inutilisés.

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

title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
```

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

L'option `intel_idle.max_cstate=1`configure la limite de l'état C pour les instances Intel, et l'option `processor.max_cstate=1` configure la limite de l'état C pour les instances basées sur AMD. Il est possible d'ajouter les deux options à votre configuration en toute sécurité. Cela permet à une configuration unique de définir le comportement souhaité sur Intel et AMD.

3. Enregistrez le fichier et quittez votre éditeur.
4. Redémarrez votre instance pour activer la nouvelle option noyau.

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

L'exemple suivant montre une instance `c4.8xlarge` avec deux cœurs qui fonctionnent activement à la fréquence « Turbo Boost » lorsque tous les cœurs sont utilisés.

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

Dans cet exemple, les cœurs des versions CPUs 19 et 28 fonctionnent à 3.2 GHz, et les autres cœurs sont à l'C1état C, en attente d'instructions. Même si les cœurs en fonctionnement n'atteignent

pas leur fréquence Turbo Boost maximale, les cœurs inactifs seront beaucoup plus rapides à répondre aux nouvelles requêtes que s'ils possédaient l'état « C-state » `C6` plus profond.

Performances de base avec les variations les plus faibles

Vous pouvez réduire les variations de la fréquence du processeur avec des états « P-states ». Les états « P-states » contrôlent les performances souhaitées (dans la fréquence de l'UC) à partir d'un cœur. La plupart des charges de travail fonctionnent mieux avec l'état P0 ce qui demande une fréquence Turbo Boost. Cependant, il se peut que vous souhaitiez adapter votre système pour obtenir une performance cohérente plus que transmise en paquets ce qui peut se produire lorsque les fréquences Turbo Boost sont activées.

Les charges de travail Intel Advanced Vector Extensions (AVX ou AVX2) peuvent fonctionner correctement à des fréquences plus basses, et les instructions AVX peuvent consommer plus d'énergie. L'exécution du processeur à une fréquence plus basse en désactivant la fréquence Turbo Boost peut réduire la quantité d'énergie utilisée et conserver la cohérence de la vitesse. Pour obtenir plus d'informations sur l'optimisation de la configuration et la charge de travail de votre instance pour AVX, consultez le site Web d'Intel.

Les pilotes inactifs du processeur contrôlent l'état P. Les nouvelles générations de CPU nécessitent des pilotes inactifs du processeur mis à jour qui correspondent au niveau du noyau, comme suit :

- Versions 6.1 et supérieures du noyau Linux : compatible avec Intel Granite Rapids (par exemple, R8i)
- Versions du noyau Linux 5.10 et supérieures : compatible avec AMD Milan (par exemple, m6A)
- Versions 5.6 et supérieures du noyau Linux : compatible avec Intel Icelake (par exemple, M6i)

Pour détecter si le noyau d'un système en cours d'exécution reconnaît le CPU, exécutez la commande suivante.

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

Si la sortie de cette commande indique un manque de prise en charge, nous vous recommandons de mettre à niveau le noyau.

Cette section décrit comment limiter les états de veille plus longs et désactiver la fréquence Turbo Boost (en demandant l'état « P-state » `P1`) pour offrir une latence faible et la variation de vitesse du processeur la plus faible pour ces types de charges de travail.

Pour limiter les états de sommeil plus profonds et désactiver Turbo Boost AL2

1. Ouvrez le fichier `/etc/default/grub` avec l'éditeur de votre choix.

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

2. Modifiez la ligne `GRUB_CMDLINE_LINUX_DEFAULT` et ajoutez l'option `intel_idle.max_cstate=1` pour `processor.max_cstate=1` définir `C1` comme l'état « C-state » le plus profond pour les cœurs inutilisés.

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

   L'option `intel_idle.max_cstate=1` configure la limite de l'état C pour les instances Intel, et l'option `processor.max_cstate=1` configure la limite de l'état C pour les instances basées sur AMD. Il est possible d'ajouter les deux options à votre configuration en toute sécurité. Cela permet à une configuration unique de définir le comportement souhaité sur Intel et AMD.

3. Enregistrez le fichier et quittez votre éditeur.
4. Exécutez la commande suivante pour recréer la configuration du démarrage.

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

5. Redémarrez votre instance pour activer la nouvelle option noyau.

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

6. Lorsque vous avez besoin des faibles variations de vitesse du processeur que l'état P-state P1 offre, exécutez la commande suivante pour désactiver la fréquence Turbo Boost.

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

7. Lorsque votre charge de travail est terminée, vous pouvez réactiver la fréquence Turbo Boost avec la commande suivante.

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

Pour limiter les états de veille plus profonds et désactiver la fréquence Turbo Boost sur Amazon Linux AMI

1. Ouvrez le fichier `/boot/grub/grub.conf` avec l'éditeur de votre choix.

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

2. Modifiez la ligne `kernel` de la première entrée et ajoutez les options `intel_idle.max_cstate=1` et `processor.max_cstate=1` pour définir `C1` comme l'état « C-state » le plus profond pour les cœurs inutilisés.

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

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

   L'option `intel_idle.max_cstate=1`configure la limite de l'état C pour les instances Intel, et l'option `processor.max_cstate=1` configure la limite de l'état C pour les instances basées sur AMD. Il est possible d'ajouter les deux options à votre configuration en toute sécurité. Cela permet à une configuration unique de définir le comportement souhaité sur Intel et AMD.

3. Enregistrez le fichier et quittez votre éditeur.
4. Redémarrez votre instance pour activer la nouvelle option noyau.

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

5. Lorsque vous avez besoin des faibles variations de vitesse du processeur que l'état P-state P1 offre, exécutez la commande suivante pour désactiver la fréquence Turbo Boost.

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

6. Lorsque votre charge de travail est terminée, vous pouvez réactiver la fréquence Turbo Boost avec la commande suivante.

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

L'exemple suivant montre une `c4.8xlarge` instance avec deux v exécutant CPUs activement un travail à la fréquence de base, sans Turbo Boost.

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

Les cœurs des versions CPUs 21 et 28 exécutent activement leur travail à la vitesse de base du processeur de 2,9 GHz, et tous les cœurs inactifs fonctionnent également à la vitesse de base dans l'`C1`état C, prêts à accepter des instructions.

Planificateur d'E/S pour AL2

Les I/O scheduler is a part of the Linux operating system that sorts and merges I/O demandes et détermine l'ordre dans lequel elles sont traitées.

I/O schedulers are particularly beneficial for devices such as magnetic hard drives, where seek time can be expensive and where it is optimal to merge co-located requests. I/Oles planificateurs ont moins d'effet sur les périphériques SSD et les environnements virtualisés. En effet, pour les

périphériques SSD, l'accès séquentiel et aléatoire ne diffère pas, et pour les environnements virtualisés, l'hôte fournit sa propre couche de planification.

Cette rubrique traite du planificateur Amazon Linux I/O . Pour plus d'informations sur le planificateur d'I/O utilisé par d'autres distributions Linux, reportez-vous à leur documentation respective.

Rubriques

Planificateurs pris en charge

Amazon Linux prend en charge les I/O planificateurs suivants :

- `deadline`— Le I/O planificateur de délais trie les I/O demandes et les traite dans l'ordre le plus efficace. Il garantit une heure de début pour chaque I/O request. It also gives I/O demande en attente depuis trop longtemps avec une priorité plus élevée.
- `cfq`— Le I/O planificateur Completely Fair Queueing (CFQ) tente de répartir I/O resources between processes. It sorts and inserts I/O équitablement les demandes dans des files d'attente par processus.
- `noop`— Les I/O scheduler inserts all I/O demandes No Operation (noop) sont placées dans une file d'attente FIFO, puis les fusionnent en une seule demande. Ce planificateur n'effectue aucun tri des demandes.

Planificateur par défaut

No Operation (noop) est le I/O planificateur par défaut pour Amazon Linux. Ce planificateur est utilisé pour les raisons suivantes :

- De nombreux types d'instance utilisent des périphériques virtualisés sur lesquels l'hôte sous-jacent effectue une planification pour l'instance.
- Les périphériques SSD sont utilisés dans de nombreux types d'instances où les avantages d'un I/O planificateur ont moins d'effet.
- C'est le I/O planificateur le moins invasif, et il peut être personnalisé si nécessaire.

Modifier le planificateur

La modification du I/O planificateur peut augmenter ou diminuer les performances selon que le planificateur entraîne le traitement d'un plus grand nombre ou d'une diminution du nombre de I/O demandes dans un délai donné. Cela dépend largement de votre charge de travail, de la génération du type d'instance utilisé et du type de périphérique auquel vous accédez. Si vous modifiez le planificateur d'E/S utilisé, nous vous recommandons d'utiliser un outil, tel que iotop, pour mesurer les I/O performances et déterminer si le changement est bénéfique pour votre cas d'utilisation.

Vous pouvez afficher le I/O planificateur d'un appareil à l'aide de la commande suivante, qui `nvme0n1` sert d'exemple. Remplacez `nvme0n1` dans la commande suivante par le périphérique répertorié dans `/sys/block` sur votre instance.

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

Pour définir le I/O planificateur de l'appareil, utilisez la commande suivante.

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

Par exemple, pour définir le I/O planificateur d'un *xvda* appareil de `noop` à`cfq`, utilisez la commande suivante.

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

Modifier le nom d'hôte de votre instance AL2

Lorsque vous lancez une instance dans un VPC privé, Amazon EC2 attribue un nom d'hôte au système d'exploitation invité. Le type de nom d'hôte attribué par Amazon dépend EC2 des paramètres de votre sous-réseau. Pour plus d'informations sur les EC2 noms d'hôtes, consultez les types de noms d'hôtes des EC2 instances Amazon dans le guide de EC2 l'utilisateur Amazon.

Un nom DNS EC2 privé Amazon typique pour une EC2 instance configurée pour utiliser une dénomination basée sur l'IP avec une IPv4 adresse ressemble à ceci : `ip-12-34-56-78.us-west-2.compute.internal` le nom comprend le domaine interne, le service (dans ce cas,`compute`), la région et une forme d' IPv4 adresse privée. Une partie de ce nom d'hôte est affiché sur l'invite shell lorsque vous vous connectez dans votre instance (par exemple, `ip-12-34-56-78`). Chaque fois que vous arrêtez et redémarrez votre EC2 instance Amazon (sauf si vous utilisez une adresse IP élastique), l' IPv4 adresse publique change, de même que votre nom DNS public, votre nom d'hôte système et votre invite shell.

> **Important**
>
> Ces informations s'appliquent à Amazon Linux. Pour obtenir des informations sur d'autres distributions, consultez leur documentation spécifique.

Modifier le nom d'hôte du système

Si vous avez un nom DNS public enregistré pour l'adresse IP de votre instance (comme `webserver.mydomain.com`), vous pouvez régler le nom d'hôte du système pour que votre instance s'identifie comme une partie de ce domaine. Cela modifie également l'invite du shell afin qu'elle affiche la première partie de ce nom au lieu du nom d'hôte fourni par AWS (par exemple,`ip-12-34-56-78`). Si vous n'avez pas de nom DNS public enregistré, vous pouvez toujours changer le nom d'hôte, mais le processus est un peu différent.

Pour que la mise à jour de votre nom d'hôte persiste, vous devez vérifier que le paramètre cloud-init `preserve_hostname` est défini sur `true`. Vous pouvez exécuter la commande suivante afin de modifier ou d'ajouter ce paramètre :

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

Si le paramètre `preserve_hostname` n'est pas répertorié, ajoutez la ligne de texte suivante à la fin du fichier :

```
preserve_hostname: true
```

Pour remplacer le nom d'hôte du système par un nom DNS public

Suivez cette procédure si vous avez déjà un nom DNS public enregistré.

1.
   - Pour AL2 : utilisez la hostnamectl commande pour définir votre nom d'hôte afin qu'il reflète le nom de domaine complet (tel que**`webserver.mydomain.com`**).

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

   - Pour Amazon Linux AMI : Sur votre instance, ouvrez le fichier de configuration `/etc/sysconfig/network` dans votre éditeur de texte et modifiez l'entrée `HOSTNAME` pour refléter le nom de domaine complet (comme **`webserver.mydomain.com`**).

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

2. Redémarrez l'instance pour récupérer le nouveau nom d'hôte.

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

Vous pouvez également redémarrer à l'aide de la EC2 console Amazon (sur la page Instances, sélectionnez l'instance et choisissez État de l'instance, Redémarrer l'instance).

3. Connectez-vous à votre instance et vérifiez que le nom d'hôte a été mis à jour. Votre invite devrait indiquer le nouveau no d'hôte (jusqu'au premier « . ») et la commande hostname doit afficher le nom de domaine complet.

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

Pour remplacer le nom d'hôte du système sans nom DNS public

1. • Pour AL2 : utilisez la hostnamectl commande pour définir votre nom d'hôte afin qu'il reflète le nom d'hôte du système souhaité (par exemple). **webserver**

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

• Pour Amazon Linux AMI : Sur votre instance, ouvrez le fichier de configuration `/etc/sysconfig/network` dans votre éditeur de texte préféré et modifiez l'entrée `HOSTNAME` pour refléter le nom d'hôte du système souhaité (comme **webserver**).

```
HOSTNAME=webserver.localdomain
```

2. Ouvrez le fichier `/etc/hosts` dans votre éditeur de texte préféré et modifiez l'entrée commençant par **127.0.0.1** pour correspondre à l'exemple ci-dessous, en remplaçant votre propre nom d'hôte.

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

3. Redémarrez l'instance pour récupérer le nouveau nom d'hôte.

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

Vous pouvez également redémarrer à l'aide de la EC2 console Amazon (sur la page Instances, sélectionnez l'instance et choisissez État de l'instance, Redémarrer l'instance).

4. Connectez-vous à votre instance et vérifiez que le nom d'hôte a été mis à jour. Votre invite devrait indiquer le nouveau no d'hôte (jusqu'au premier « . ») et la commande hostname doit afficher le nom de domaine complet.

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

Vous pouvez également implémenter des solutions plus programmatiques, telles que la spécification des données utilisateur pour configurer votre instance. Si votre instance fait partie d'un groupe Auto Scaling, vous pouvez utiliser des hooks de cycle de vie pour définir les données utilisateur. Pour de plus amples informations, veuillez consulter les rubriques Run commands on your Linux instance at launch (Exécution des commandes sur votre instance Linux lors de son lancement) et Lifecycle hook for instance launch (Hook de cycle de vie pour le lancement d'instance) dans le Guide de l'utilisateur AWS CloudFormation .

Modifier l'invite shell sans affecter le nom d'hôte

Si vous ne souhaitez pas modifier le nom d'hôte de votre instance, mais que vous souhaitez afficher un nom de système plus utile (tel que**webserver**) que le nom privé fourni par AWS (par exemple,`ip-12-34-56-78`), vous pouvez modifier les fichiers de configuration des invites du shell pour afficher le surnom de votre système au lieu du nom d'hôte.

Pour remplacer l'invite shell par un pseudonyme d'hôte

1. Créez un fichier dans `/etc/profile.d` qui définit la variable d'environnement appelée `NICKNAME` avec la valeur que vous souhaitez dans l'invite shell. Par exemple, pour définir le pseudonyme du système sur **webserver**, exécutez la commande suivante.

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

2. Ouvrez le fichier `/etc/bashrc` (Red Hat) ou `/etc/bash.bashrc` (Debian/Ubuntu) dans l'éditeur de texte de votre choix (par exemple, vim ou nano). Vous devez utiliser sudo avec la commande de l'éditeur, car `/etc/bashrc` et `/etc/bash.bashrc` appartiennent à `root`.

3. Modifiez le fichier et changez la variable d'invite shell (PS1) pour afficher votre pseudonyme au lieu du nom d'hôte. Recherchez la ligne suivante qui définit l'invite shell dans `/etc/bashrc` ou `/etc/bash.bashrc` (plusieurs lignes sont affichées ci-dessous pour illustrer le contexte ; recherchez la ligne qui commence par `[ "$PS1"`) :

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

   Modifiez \h (symbole de `hostname`) sur cette ligne en la valeur de la variable `NICKNAME`.

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

4. (Facultatif) Pour définir le titre sur les fenêtres shell avec le nouveau pseudonyme, suivez les étapes suivantes.

   a. Créez un fichier nommé `/etc/sysconfig/bash-prompt-xterm`.

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

   b. Rendez le fichier exécutable avec la commande suivante.

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

   c. Ouvrez le fichier `/etc/sysconfig/bash-prompt-xterm` avec votre éditeur de texte préféré (comme vim ou nano). Vous devez utiliser sudo avec la commande de votre éditeur, car `/etc/sysconfig/bash-prompt-xterm` est détenu par `root`.

   d. Ajoutez la ligne suivante au fichier.

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

5. Déconnectez-vous puis reconnectez-vous pour récupérer la nouvelle valeur du pseudonyme.

Modifier le nom d'hôte sur d'autres distributions Linux

Les procédures de cette page sont destinées à une utilisation avec Amazon Linux uniquement. Pour plus d'informations sur les autres distributions Linux, consultez leur documentation spécifique et les articles suivants :

- Comment attribuer un nom d'hôte statique à une EC2 instance Amazon privée exécutant RHEL 7 ou Centos 7 ?

Configurer le DNS dynamique sur votre AL2 instance

Lorsque vous lancez une EC2 instance, une adresse IP publique et un nom de système de noms de domaine (DNS) lui sont attribués, que vous pouvez utiliser pour y accéder depuis Internet. Comme il y a tellement d'hôtes dans le domaine Amazon Web Services, ces noms publics doivent être assez longs pour que chaque nom reste unique. Un nom DNS EC2 public Amazon typique ressemble à ceci : `ec2-12-34-56-78.us-west-2.compute.amazonaws.com` le nom comprend le domaine Amazon Web Services, le service (dans ce cas,`compute`), le Région AWS, et une forme d'adresse IP publique.

Les services DNS dynamiques fournissent des noms d'hôte DNS personnalisés dans leur domaine qui peut être facile à mémoriser et aussi plus pertinent vis-à-vis du cas d'utilisation de votre hôte. Certains de ces services sont également gratuits. Vous pouvez utiliser un fournisseur DNS dynamique avec Amazon EC2 et configurer l'instance pour mettre à jour l'adresse IP associée à un nom DNS public à chaque démarrage de l'instance. Il existe un choix de plusieurs fournisseurs différents et les détails spécifiques à la sélection d'un fournisseur et à l'enregistrement d'un nom sans eux ne sont pas pris en compte dans le cadre de ce guide.

Pour utiliser le DNS dynamique avec Amazon EC2

1. Inscrivez-vous avec un fournisseur de services DNS dynamiques et enregistrez un nom DNS public avec leur service. Cette procédure utilise le service gratuit de noip.com/free comme exemple.
2. Configurez le client de mise à jour de DNS dynamique. Après avoir enregistré un fournisseur de services DNS dynamiques et un nom DNS public avec leur service, reliez le nom DNS à l'adresse IP de votre instance. De nombreux fournisseurs (notamment noip.com) vous permettent de faire cela manuellement depuis la page de votre compte sur leur site web, mais beaucoup prennent également en charge les clients de mise à jour logicielle. Si un client de mise à jour est en cours d'exécution sur votre EC2 instance, votre enregistrement DNS dynamique

est mis à jour chaque fois que l'adresse IP change, comme c'est le cas après un arrêt et un redémarrage. Dans cet exemple, vous installez le client noip2 qui fonctionne avec le service fourni par noip.com.

a. Activez le référentiel Extra Packages for Enterprise Linux (EPEL) pour accéder au `noip2` client.

> **Note**
>
> AL2 les clés GPG et les informations de référentiel du référentiel EPEL sont installées par défaut sur les instances. Pour plus d'informations et pour télécharger la dernière version de ce package, consultez https://fedoraproject. org/wiki/EPEL.

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

b. Installez le package `noip`.

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

c. Créez le fichier de configuration . Saisissez l'identifiant et le mot de passe lorsque vous y êtes invité et répondez aux questions suivantes pour configurer le client.

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

3. Activez le service noip.

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

4. Lancez le service noip.

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

Cette commande lance le client, qui lit le fichier de configuration (`/etc/no-ip2.conf`) que vous avez créé précédemment et met à jour l'adresse IP du nom du DNS public que vous avez choisi.

5. Vérifiez que le client de mise à jour a défini la bonne adresse IP de votre nom DNS dynamique. Laissez s'écouler quelques minutes pour que les enregistrements DNS se mettent à jour, puis

essayez de connecter votre instance en utilisant SSH avec le nom DNS public que vous avez configuré dans cette procédure.

Configurez votre interface réseau à l'aide d'ec2-net-utils pour AL2

Amazon Linux 2 AMIs peut contenir des scripts supplémentaires installés par AWS, appelés ec2-net-utils. Ces scripts automatisent le cas échéant la configuration de vos interfaces réseau. Ces scripts ne sont disponibles AL2 que pour.

> **Note**
>
> Pour Amazon Linux 2023, le `amazon-ec2-net-utils` package génère des configurations spécifiques à l'interface dans le répertoire. `/run/systemd/network` Pour plus d'informations, consultez la rubrique Networking service du Guide de l'utilisateur Amazon Linux 2023.

Utilisez la commande suivante pour installer le package AL2 s'il n'est pas déjà installé ou pour le mettre à jour s'il est installé et que des mises à jour supplémentaires sont disponibles :

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

Les composants suivants font partie de ec2-net-utils :

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

Identifie les interfaces réseau qui sont attachées, détachées ou rattachées à une instance en cours d'exécution, et s'assure que le script hotplug s'exécute (`53-ec2-network-interfaces.rules`). Mappe l'adresse MAC sur un nom de périphérique (`75-persistent-net-generator.rules`, qui génère `70-persistent-net.rules`).

script hotplug

Génère un fichier de configuration d'interface adapté à une utilisation avec DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Génère également un fichier de configuration de route (`/etc/sysconfig/network-scripts/route-ethN`).

script DHCP

Chaque fois qu'une Network Interface reçoit un nouveau bail DHCP, ce script interroge les métadonnées d'instance pour des adresses IP Elastic. Pour chaque adresse IP Elastic, il ajoute une règle à la base de données de politiques de routage pour s'assurer que le trafic sortant à partir de cette adresse utilise l'interface réseau correcte. Il ajoute également chaque adresse IP privée à l'interface réseau comme adresse secondaire.

ec2ifup ethN (`/usr/sbin/`)

Étend la fonctionnalité de la commande standard ifup. Une fois que ce script a réécrit les fichiers de configuration `ifcfg-ethN` et `route-ethN`, il exécute ifup.

ec2ifdown ethN (`/usr/sbin/`)

Étend la fonctionnalité de la commande standard ifdown. Une fois que le script a supprimé les règles pour l'interface réseau de la base de données des stratégies de routage, il exécute ifdown.

ec2ifscan (`/usr/sbin/`)

Recherche les interfaces réseau qui n'ont pas été configurées et les configure.

Ce script n'est pas disponible dans la version initiale de ec2-net-utils.

Pour répertorier les fichiers de configuration générés par ec2-net-utils, utilisez la commande suivante :

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

Pour désactiver l'automatisation, vous pouvez ajouter `EC2SYNC=no` au fichier `ifcfg-ethN` correspondant. Par exemple, utilisez la commande suivante pour désactiver l'automatisation pour l'interface eth1 :

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

Pour désactiver complètement l'automatisation, vous pouvez supprimer le package à l'aide de la commande suivante :

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

Noyaux fournis par l'utilisateur

Si vous avez besoin d'un noyau personnalisé sur vos EC2 instances Amazon, vous pouvez commencer par une AMI proche de ce que vous souhaitez, compiler le noyau personnalisé sur votre instance et mettre à jour le chargeur de démarrage pour qu'il pointe vers le nouveau noyau. Ce processus varie en fonction du type de virtualisation qu'utilise votre AMI. Pour plus d'informations, consultez les types de virtualisation d'AMI Linux dans le guide de EC2 l'utilisateur Amazon.

Table des matières

HVM AMIs (GRUB)

Les volumes d'instance HVM sont traités comme des disques physiques réels. Le processus de démarrage est similaire à celui d'un système d'exploitation bare metal avec disque partitionné et programme d'amorçage, ce qui lui permet de travailler avec toutes les distributions Linux actuellement prises en charge. Le bootloader le plus courant est GRUB ou. GRUB2

Par défaut, GRUB n'envoie pas ses données de sortie à la console de l'instance car il crée un délai de démarrage supplémentaire. Pour plus d'informations, consultez la sortie de la console Instance dans le guide de EC2 l'utilisateur Amazon. Si vous installez un noyau personnalisé, vous devez envisager d'activer la sortie GRUB.

Vous n'avez pas besoin de spécifier un noyau de rechange, mais nous vous recommandons d'en avoir un lorsque vous testez un nouveau noyau. GRUB peut avoir recours à un autre noyau au cas où le nouveau noyau échoue. Le fait d'avoir un noyau de rechange permet à l'instance de démarrer même si le nouveau noyau n'est pas trouvé.

L'ancien GRUB pour Amazon Linux est utilisé`/boot/grub/menu.lst`. GRUB2 pour les AL2 usages`/etc/default/grub`. Pour plus d'informations sur la mise à jour du noyau par défaut dans le chargeur d'amorçage, consultez la documentation de votre distribution Linux.

Paravirtuel AMIs (PV-GRUB)

AMIs qui utilisent la virtualisation paravirtuelle (PV) utilisent un système appelé PV-GRUB pendant le processus de démarrage. PV-GRUB est un programme d'amorçage paravirtuel qui exécute une version corrigée de GNU GRUB 0.97. Lorsque vous lancez une instance, PV-GRUB commence le

processus de démarrage, puis charge en chaîne le noyau spécifié par le fichier `menu.lst` de votre image.

PV-GRUB comprend les commandes `grub.conf` ou `menu.lst` standard qui lui permettent de fonctionner avec toutes les distributions Linux actuellement prises en charge. Les distributions plus anciennes comme Ubuntu 10.04 LTS, Oracle Enterprise Linux ou CentOS 5.x ont besoin d'un package noyau spécial « ec2 » ou « xen » alors les distributions les plus récentes comprennent les pilotes nécessaires dans le package noyau par défaut.

La plupart des systèmes paravirtuels modernes AMIs utilisent une API PV-GRUB par défaut (y compris tous les Linux paravirtuels disponibles dans AMIs le menu de démarrage rapide d'Amazon Launch EC2 Wizard). Vous n'avez donc aucune étape supplémentaire à suivre pour utiliser un noyau différent sur votre instance, à condition que le noyau que vous souhaitez utiliser soit compatible avec votre distribution. La meilleure façon d'exécuter un noyau personnalisé sur une instance est de commencer avec une AMI qui est proche de ce que vous voulez, puis de compiler le noyau personnalisé sur votre instance et de modifier le fichier `menu.lst` pour démarrer avec ce noyau.

Vous pouvez vérifier que l'image du noyau d'une AMI est un AKI PV-GRUB. Exécutez la commande describe-images suivante (en indiquant votre ID d'image de noyau) et vérifiez que le champ `Name` commence par `pv-grub` :

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

Sommaire

Restrictions de PV-GRUB

PV-GRUB possède les restrictions suivantes :

- Vous ne pouvez pas utiliser la version 64 bit de PV-GRUB pour lancer un noyau 32 bits ou vice versa.
- Vous ne pouvez pas spécifier une image ramdisk Amazon (ARI) lorsque vous utilisez une PV-GRUB AKI.

- AWS a testé et vérifié que PV-GRUB fonctionne avec les formats de système de fichiers suivants : EXT2,,, JFS EXT3 EXT4, XFS et ReiserFS. Il se peut que d'autres formats de système de fichiers ne fonctionnent pas.
- PV-GRUB peut démarrer les noyaux compressés à l'aide de formats de compression gzip, bzip2, lzo et xz.
- Les clusters AMIs ne prennent pas en charge ou n'ont pas besoin de PV-GRUB, car ils utilisent la virtualisation matérielle complète (HVM). Tandis que les instances paravirtuelles utilisent PV-GRUB pour le démarrage, les volumes d'instances HVM sont traités comme de véritables disques et le processus de démarrage est similaire au processus de démarrage d'un système d'exploitation bare metal avec un disque divisé et un chargeur de démarrage.
- Les versions PV-GRUB 1.03 et antérieures ne prennent pas en charge le partitionnement GPT. Elles prennent uniquement en charge le partitionnement MBR.
- Si vous comptez utiliser un gestionnaire par volumes logiques (LVM) avec des volumes Amazon Elastic Block Store (Amazon EBS), vous avez besoin d'une partition de démarrage séparée externe au LVM. Puis, vous pouvez créer des volumes logiques avec le LVM.

Configurer GRUB pour le paravirtual AMIs

Pour démarrer PV-GRUB, un fichier `menu.lst` GRUB doit exister dans l'image. L'emplacement le plus commun de ce fichier est `/boot/grub/menu.lst`.

Ce qui suit est un exemple d'un fichier de configuration `menu.lst` pour le démarrage d'une AMI avec une AKI PV-GRUB. Dans cet exemple, un choix de deux entées noyau est proposé : Amazon Linux 03/2018 (le noyau original pour cette AMI) et Vanilla Linux 4.16.4 (une version plus récente du noyau Vanilla Linux de https://www.kernel.org/). L'entrée Vanilla a été copiée de l'entrée originale pour cette AMI et les chemins `kernel` et `initrd` ont été mis à jour par rapport aux nouveaux emplacements. Le paramètre `default 0` pointe le programme d'amorçage vers la première entrée qu'il voit (dans ce cas, l'entrée Vanilla) et le paramètre `fallback 1` pointe le programme d'amorçage vers la prochaine entrée s'il existe un problème lors du démarrage du premier.

```
default 0
fallback 1
timeout 0
hiddenmenu

title Vanilla Linux 4.16.4
root (hd0)
```

```
kernel /boot/vmlinuz-4.16.4 root=LABEL=/ console=hvc0
initrd /boot/initrd.img-4.16.4

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

Vous ne devez pas spécifier un noyau de rechange dans votre fichier `menu.lst`, mais nous vous recommandons d'en avoir un lorsque vous tester un nouveau noyau. PV-GRUB peut avoir recours à un autre noyau au cas où le nouveau noyau échoue. Le fait d'avoir un noyau de rechange permet à l'instance de démarrer même si le nouveau noyau n'est pas trouvé.

PV-GRUB vérifie les emplacements suivants pour `menu.lst` en utilisant le premier qu'il trouve :

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

Notez que les versions PV-GRUB 1.03 et antérieures ne vérifient que l'un des deux premiers emplacements de cette liste.

Image du noyau Amazon PV-GRUB IDs

Les PV-GRUB AKIs sont disponibles dans toutes les EC2 régions d'Amazon, à l'exception de l'Asie-Pacifique (Osaka). Il existe AKIs des types d'architecture 32 bits et 64 bits. La plupart des modèles modernes AMIs utilisent un PV-GRUB AKI par défaut.

Nous vous recommandons de toujours utiliser la dernière version de l'AKI PV-GRUB, car les versions de l'AKI PV-GRUB ne sont pas toutes compatibles avec les types d'instance. Utilisez la commande describe-images suivante pour obtenir la liste des PV-GRUB AKIs pour la région actuelle :

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

PV-GRUB est la seule AKI disponible dans la région `ap-southeast-2`. Vous devriez vérifier que toutes les AMI que vous voulez copier vers cette région utilisent une version de PV-GRUB qui est disponible dans cette région.

Voici l'AKI actuel IDs pour chaque région. Enregistrez un nouveau fichier AMIs à l'aide d'un HD0 AKI.

> **Note**
>
> Nous continuons à fournir le hd00 à AKIs des fins de rétrocompatibilité dans les régions où il était auparavant disponible.

ap-northeast-1, Asia Pacific (Tokyo)

ID de l'image	Nom de l'image
`aki-f975a998`	`pv-grub-hd0_1.05-i386.gz`
`aki-7077ab11`	`pv-grub-hd0_1.05-x86_64.gz`

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

ID de l'image	Nom de l'image
`aki-17a40074`	`pv-grub-hd0_1.05-i386.gz`
`aki-73a50110`	`pv-grub-hd0_1.05-x86_64.gz`

ap-southeast-2, Asia Pacific (Sydney)

ID de l'image	Nom de l'image
`aki-ba5665d9`	`pv-grub-hd0_1.05-i386.gz`
`aki-66506305`	`pv-grub-hd0_1.05-x86_64.gz`

eu-central-1, Europe (Frankfurt)

ID de l'image	Nom de l'image
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1, Europe (Ireland)

ID de l'image	Nom de l'image
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1, South America (São Paulo)

ID de l'image	Nom de l'image
aki-7cd34110	pv-grub-hd0_1.05-i386.gz
aki-912fbcfd	pv-grub-hd0_1.05-x86_64.gz

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

ID de l'image	Nom de l'image
aki-04206613	pv-grub-hd0_1.05-i386.gz
aki-5c21674b	pv-grub-hd0_1.05-x86_64.gz

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

ID de l'image	Nom de l'image
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz

ID de l'image	Nom de l'image
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

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

ID de l'image	Nom de l'image
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2, US West (Oregon)

ID de l'image	Nom de l'image
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

Mise à jour PV-GRUB

Nous vous recommandons de toujours utiliser la dernière version de l'AKI PV-GRUB, car les versions de l'AKI PV-GRUB ne sont pas toutes compatibles avec les types d'instance. De plus, les versions les plus anciennes de PV-GRUB ne sont pas disponibles dans toutes les régions. Si vous copiez une AMI qui utilise une version plus ancienne pour une région que ne prend pas en charge cette version, vous ne pourrez donc pas démarrer des instances lancées à partir d'une AMI jusqu'à ce que vous mettiez à jour l'image noyau. Utilisez les procédures suivantes pour vérifier la version de PV-GRUB de votre instance et la mettre à jour si nécessaire.

Pour vérifier votre version de PV-GRUB

1. Trouvez l'ID noyau pour votre instance.

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

{
```

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

L'ID noyau pour cette instance est `aki-70cb0e10`.

2. Consultez les informations sur la version de cet ID noyau.

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

{
    "Images": [
        {
            "VirtualizationType": "paravirtual",
            "Name": "pv-grub-hd0_1.05-x86_64.gz",
            ...
            "Description": "PV-GRUB release 1.05, 64-bit"
        }
    ]
}
```

Cette image noyau est PV-GRUB 1.05. Si votre version PV-GRUB n'est pas la plus récente (comme indiqué dans le didacticiel Image du noyau Amazon PV-GRUB IDs), vous devriez la mettre à jour en suivant la procédure ci-dessous.

Pour mettre à jour votre version de PV-GRUB

Si votre instance utilise une version de PV-GRUB plus ancienne, vous devriez la mettre à jour.

1. Identifiez le dernier PV-GRUB AKI pour votre région et l'architecture de processeur à partir de Image du noyau Amazon PV-GRUB IDs.
2. Arrêtez votre instance. Votre instance doit être arrêtée pour modifier l'image noyau utilisée.

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

3. Modifiez l'image noyau utilisée pour votre instance.

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

4. Redémarrez votre instance.

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

AL2 Notifications de publication de l'AMI

Pour être informé de la sortie de nouveaux Amazon Linux AMIs , vous pouvez vous abonner via Amazon SNS.

Pour plus d'informations sur l'abonnement aux notifications pour AL2 2023, consultez la section Recevoir des notifications sur les nouvelles mises à jour dans le guide de l'utilisateur Amazon Linux 2023.

> **Note**
>
> Le support standard pour AL1 a pris fin le 31 décembre 2020. La phase AL1 de support de maintenance s'est terminée le 31 décembre 2023. Pour plus d'informations sur l' AL1 EOL et le support de maintenance, consultez le billet de blog Update on Amazon Linux AMI end-of-life.

Pour s'abonner aux notifications Amazon Linux

1. Ouvrez la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner la région dans laquelle la notification SNS à laquelle vous vous abonnez a été créée.
3. Dans le panneau de navigation, choisissez Abonnements, puis Créer un abonnement.
4. Dans la boîte de dialogue Créer un abonnement, procédez comme suit :
   a. [AL2] Pour ARN de la rubrique, copiez et collez l'Amazon Resource Name (ARN) suivant : **`arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates`**.
   b. [Amazon Linux] Pour ARN de la rubrique, copiez et collez l'Amazon Resource Name (ARN) suivant : **`arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates`**.
   c. Pour Protocole, choisissez E-mail.
   d. Pour Point de terminaison, entrez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.

e. Choisissez Créer un abonnement.

5. Vous recevez un e-mail de confirmation dont l'objet est « AWS Notification - Confirmation d'abonnement ». Ouvrez l'e-mail et choisissez Confirm subscription (Confirmer l'abonnement) pour terminer votre abonnement.

Chaque fois qu' AMIs elles sont publiées, nous envoyons des notifications aux abonnés du sujet correspondant. Pour arrêter de recevoir ces notifications, utilisez la procédure suivante pour vous désabonner.

Pour annuler votre abonnement aux notifications Amazon Linux

1. Ouvrez la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez utiliser la région dans laquelle la notification SNS a été créée.
3. Dans le panneau de navigation, sélectionnez Abonnements, sélectionnez l'abonnement, puis Actions, Supprimer des abonnements.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Format du message Amazon Linux AMI SNS

Le schéma du message SNS est le suivant.

```
{
    "description": "Validates output from AMI Release SNS message",
    "type": "object",
    "properties": {
        "v1": {
            "type": "object",
            "properties": {
                "ReleaseVersion": {
                    "description": "Major release (ex. 2018.03)",
                    "type": "string"
                },
                "ImageVersion": {
                    "description": "Full release (ex. 2018.03.0.20180412)",
                    "type": "string"
                },
                "ReleaseNotes": {
                    "description": "Human-readable string with extra information",
```

```
                    "type": "string"
                },
                "Regions": {
                    "type": "object",
                    "description": "Each key will be a region name (ex. us-east-1)",
                    "additionalProperties": {
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "Name": {
                                    "description": "AMI Name (ex. amzn-ami-
hvm-2018.03.0.20180412-x86_64-gp2)",
                                    "type": "string"
                                },
                                "ImageId": {
                                    "description": "AMI Name (ex.ami-467ca739)",
                                    "type": "string"
                                }
                            },
                            "required": [
                                "Name",
                                "ImageId"
                            ]
                        }
                    }
                }
            },
            "required": [
                "ReleaseVersion",
                "ImageVersion",
                "ReleaseNotes",
                "Regions"
            ]
        }
    },
    "required": [
        "v1"
    ]
}
```

Configuration de la connexion au bureau AL2 MATE

L'environnement de bureau MATE est préinstallé et préconfiguré AMIs avec la description suivante :

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

L'environnement fournit une interface utilisateur graphique intuitive pour administrer les instances AL2 en ayant très peu recours à la ligne de commande. L'interface utilise des représentations graphiques, telles que des icônes, des fenêtres, des barres d'outils, des dossiers, des fonds d'écran et des widgets de bureau. Des outils intégrés basés sur l'interface graphique sont disponibles pour effectuer des tâches courantes. Par exemple, il existe des outils pour ajouter et supprimer des logiciels, appliquer des mises à jour, organiser des fichiers, lancer des programmes et surveiller l'intégrité du système.

Important

`xrdp` est le logiciel de bureau à distance fourni dans l'AMI. Par défaut, `xrdp` utilise un certificat TLS auto-signé pour chiffrer les sessions de bureau à distance. AWS Ni les `xrdp` responsables ne recommandent d'utiliser des certificats auto-signés en production. Au lieu de cela, procurez-vous un certificat auprès d'une autorité de certification appropriée et installez-le sur vos instances. Pour plus d'informations sur la configuration TLS, consultez la rubrique Couche de sécurité TLS sur le wiki `xrdp`.

Note

Si vous préférez utiliser un service VNC (Virtual Network Computing) au lieu de xrdp, consultez l'article Comment installer une interface graphique sur mon EC2 instance Amazon exécutant le AL2 AWS Knowledge Center.

Prérequis

Pour exécuter les commandes présentées dans cette rubrique, vous devez installer le AWS Command Line Interface (AWS CLI) ou AWS Tools for Windows PowerShell, et configurer votre AWS profil.

Options

1. Installer le AWS CLI — Pour plus d'informations, consultez la section Installation des principes de base de la configuration AWS CLI et du guide de AWS Command Line Interface l'utilisateur.
2. Installation des outils pour Windows PowerShell : pour plus d'informations, consultez la section Installation des informations d'identification AWS Tools for Windows PowerShell et des informations d'identification partagées dans le guide de Outils AWS pour PowerShell l'utilisateur.

> **Tip**
>
> Au lieu de procéder à une installation complète du AWS CLI, vous pouvez utiliser AWS CloudShellun shell pré-authentifié basé sur un navigateur qui se lance directement depuis le. AWS Management Console Vérifiez le Régions AWS support pour vous assurer qu'il est disponible dans la région dans laquelle vous travaillez.

Configurer la connexion RDP

Procédez comme suit pour configurer une connexion RDP (Remote Desktop Protocol) à partir de votre ordinateur local vers une instance AL2 exécutant l'environnement de bureau MATE.

1. Pour obtenir l'ID de l'AMI AL2 dont le nom inclut MATE, vous pouvez utiliser la commande describe-images depuis votre outil de ligne de commande local. Si vous n'avez pas installé les outils de ligne de commande, vous pouvez exécuter la requête suivante directement depuis une AWS CloudShell session. Pour plus d'informations sur le lancement d'une session shell depuis CloudShell, consultez Getting started with AWS CloudShell. Depuis la EC2 console Amazon, vous pouvez trouver l'AMI incluse dans Mate en lançant une instance, puis `MATE` en entrant dans la barre de recherche de l'AMI. Le AL2 Quick Start avec MATE préinstallé apparaîtra dans les résultats de recherche.

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

```
    ],
    [
        "ami-0456example0def34",
        "amzn2-x86_64-MATEDE_DOTNET-2020.04.14",
        "Amazon Linux 2 with .Net Core, PowerShell, Mono, and MATE Desktop
 Environment"
    ]
]
```

Choisir l'AMI qui convient à votre utilisation.

2. Lancez une EC2 instance avec l'AMI que vous avez localisée à l'étape précédente. Configurez le groupe de sécurité pour autoriser le trafic TCP entrant vers le port 3389. Pour plus d'informations sur les groupes de sécurité, consultez Groupes de sécurité pour votre VPC. Cette configuration vous permet d'utiliser un client RDP pour vous connecter à l'instance.
3. Connectez-vous à l'instance à l'aide de SSH.
4. Mettez à jour le logiciel et le noyau de l'instance.

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

Une fois la mise à jour terminée, redémarrez l'instance pour vous assurer qu'elle utilise les derniers packages et bibliothèques de la mise à jour ; les mises à jour du noyau ne sont pas chargées jusqu'au prochain redémarrage.

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

5. Reconnectez-vous à l'instance et exécutez la commande suivante sur votre instance Linux pour définir le mot de passe pour `ec2-user`.

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

6. Installez le certificat et la clé.

Si vous disposez déjà d'un certificat et d'une clé, copiez-les dans le répertoire `/etc/xrdp/` comme suit :

- Certificat — `/etc/xrdp/cert.pem`
- Clé : `/etc/xrdp/key.pem`

Si vous ne possédez pas de certificat et de clé, utilisez la commande suivante pour les générer dans le répertoire `/etc/xrdp`.

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

> **Note**
>
> Cette commande génère un certificat valide pendant 365 jours.

7. Ouvrez un client RDP sur l'ordinateur à partir duquel vous vous connecterez à l'instance (par exemple, Connexion Bureau à distance sur un ordinateur sous Microsoft Windows). Saisissez `ec2-user` comme nom d'utilisateur et entrez le mot de passe que vous avez défini à l'étape précédente.

Pour désactiver **`xrdp`** sur votre EC2 instance Amazon

Vous pouvez désactiver `xrdp` à tout moment en exécutant l'une des commandes suivantes sur votre instance Linux. Les commandes suivantes n'ont aucune incidence sur votre capacité à utiliser MATE à l'aide d'un serveur X11.

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

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

Pour activer **`xrdp`** sur votre EC2 instance Amazon

Pour le réactiver `xrdp` afin de pouvoir vous connecter à votre AL2 instance exécutant l'environnement de bureau MATE, exécutez l'une des commandes suivantes sur votre instance Linux.

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

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

AL2 Tutoriels

Les didacticiels suivants vous montrent comment effectuer des tâches courantes à l'aide d' EC2 instances Amazon en cours d'exécution AL2. Pour les didacticiels vidéo, voir Vidéos AWS pédagogiques et ateliers.

Pour les instructions AL2 023, consultez les didacticiels du guide de l'utilisateur Amazon Linux 2023.

Tutoriels

- Tutoriel : Installation d'un serveur LAMP sur AL2
- Tutoriel : Configuration SSL/TLS sur AL2
- Tutoriel : héberger un WordPress blog sur AL2

Tutoriel : Installation d'un serveur LAMP sur AL2

Les procédures suivantes vous aident à installer un serveur Web Apache compatible avec PHP et MariaDB (un fork de MySQL développé par la communauté) AL2 sur votre instance (parfois appelé serveur Web LAMP ou stack LAMP). Vous pouvez utiliser ce serveur pour héberger un site web statique ou déployer une application PHP dynamique qui lit et écrit des informations sur une base de données.

> **Important**
>
> Si vous essayez de configurer un serveur Web LAMP sur une autre distribution, comme Ubuntu ou Red Hat Enterprise Linux, ce tutoriel ne fonctionnera pas. Pour AL2 023, voir Installer un serveur LAMP sur AL2 023. Pour Ubuntu, consultez la documentation de la communauté Ubuntu suivante : ApacheMySQLPHP. Pour les autres distributions, consultez leur documentation spécifique.

Option : Effectuer ce tutoriel en utilisant Automation

Pour terminer ce didacticiel en utilisant AWS Systems Manager Automation au lieu des tâches suivantes, exécutez le AWS document Docs-Install ALAMPServer - AL2 Automation.

Tâches

- Étape 1 : Préparer le serveur LAMP

Étape 1 : Préparer le serveur LAMP

Conditions préalables

- Ce didacticiel suppose que vous avez déjà lancé une nouvelle instance en utilisant AL2, avec un nom DNS public accessible depuis Internet. Pour plus d'informations, consultez Lancer une instance dans le guide de EC2 l'utilisateur Amazon. Vous devez aussi avoir configuré votre groupe de sécurité pour permettre les connexions SSH (port 22), HTTP (port 80) et HTTPS (port 443). Pour plus d'informations sur ces prérequis, consultez la section Règles relatives aux groupes de sécurité dans le guide de EC2 l'utilisateur Amazon.
- La procédure suivante installe la dernière version de PHP actuellement `php8.2` disponible sur AL2. Si vous prévoyez d'utiliser d'autres applications PHP que celles décrites dans ce didacticiel, vous pouvez vérifier qu'elles sont compatibles avec `php8.2`.

Pour préparer le serveur LAMP

1. Connectez-vous à votre instance.
2. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance. Ce processus peut prendre quelques minutes, mais il est important pour vous assurer que vous disposez des dernières mises à jour de sécurité et des nouveaux correctifs de bogues.

   L'option `-y` installe les mises à jour sans demander de confirmation. Si vous souhaitez examiner les mises à jour avant l'installation, vous pouvez omettre cette option.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```
3. Installez les référentiels supplémentaires Amazon Linux `mariadb10.5` pour obtenir la dernière version du package MariaDB.

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

Si vous recevez l'erreur `sudo: amazon-linux-extras: command not found`, votre instance n'a pas été lancée avec une AMI Amazon Linux 2 (vous utilisez peut-être l'AMI Amazon Linux). Vous pouvez afficher votre version d'Amazon Linux avec la commande suivante

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

4. Installez les référentiels `php8.2` Amazon Linux Extras pour obtenir la dernière version du PHP package pour AL2.

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

5. Maintenant que votre instance est à jour, vous pouvez installer le serveur web Apache, MariaDB et les packages logiciels PHP. Utilisez la commande yum install pour installer plusieurs packages logiciels et toutes les dépendances associées au même moment.

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

Vous pouvez afficher les versions actuelles de ces packages avec la commande suivante :

```
yum info package_name
```

6. Démarrez le serveur web Apache.

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

7. Utilisez la commande systemctl pour configurer le serveur Web Apache afin qu'il soit lancé à chaque démarrage système.

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

Vous pouvez vérifier que httpd est activé en exécutant la commande suivante :

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

8. Ajoutez une règle de sécurité pour autoriser les connexions HTTP entrantes (port 80) à votre instance si vous ne l'avez pas déjà fait. Par défaut, un groupe de *N* sécurité avec assistant de

lancement a été configuré pour votre instance lors de l'initialisation. Ce groupe contient une règle unique pour autoriser les connexions SSH.

a. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

b. Choisissez instances et sélectionnez votre instance.

c. Sous l'onglet Sécurité, affichez les règles entrantes. Vous devriez voir la règle suivante :

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

> **Warning**
>
> L'utilisation `0.0.0.0/0` permet à toutes les IPv4 adresses d'accéder à votre instance via SSH. Cette solution est acceptable pour une brève durée dans un environnement de test, mais n'est pas sécurisée pour les environnements de production. Dans un environnement de production, vous autorisez uniquement l'accès à votre instance pour une adresse IP ou une plage d'adresses spécifiques.

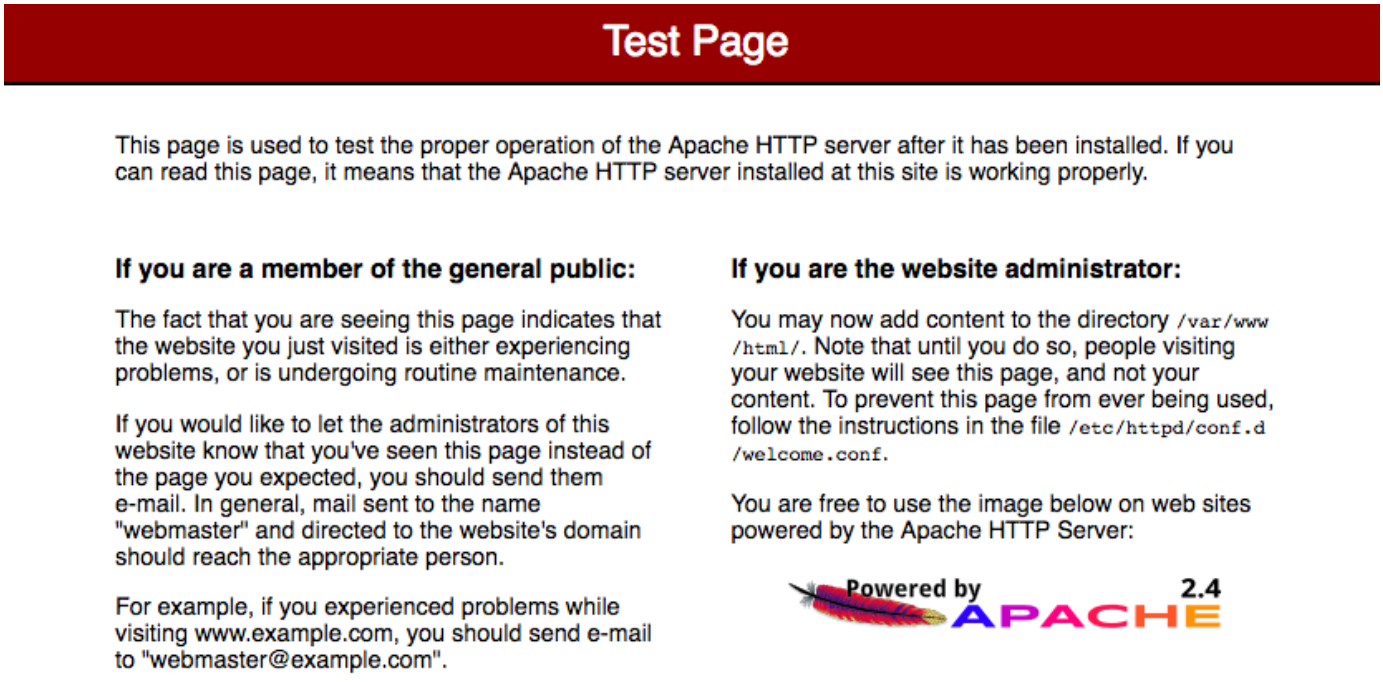
d. Choisissez le lien pour le groupe de sécurité. À l'aide des procédures décrites dans Ajouter des règles à un groupe de sécurité, ajoutez une nouvelle règle de sécurité entrante avec les valeurs suivantes :

- Type : HTTP
- Protocole : TCP
- Plage de ports : 80
- Source : Personnalisé

9. Testez votre serveur web. Dans un navigateur web, saisissez l'adresse DNS publique (ou l'adresse IP publique) de votre instance. S'il n'existe aucun contenu dans `/var/www/html`, vous devriez voir la page test Apache. Vous pouvez obtenir le DNS public de votre instance à l'aide de la EC2 console Amazon (vérifiez la colonne Public DNS ; si cette colonne est masquée, choisissez Afficher/Masquer les colonnes (l'icône en forme d'engrenage) et choisissez Public DNS).

   Vérifiez que le groupe de sécurité de l'instance contient une règle autorisant le trafic HTTP sur le port 80. Pour plus d'informations, voir Ajouter des règles au groupe de sécurité.

> **Important**
>
> Si vous n'utilisez pas Amazon Linux, il se peut que vous deviez aussi configurer le pare-feu sur votre instance pour autoriser ces connexions. Pour obtenir plus d'informations sur la configuration du pare-feu, consultez la documentation de votre distribution spécifique.



La commande httpd traite les fichiers qui sont conservés dans un répertoire appelé racine du document Apache. La racine du document Apache d'Amazon Linux est `/var/www/html` qui est détenu par défaut par la racine.

Pour autoriser le compte `ec2-user` à manipuler les fichiers de ce répertoire, vous devez modifier la propriété et les autorisations du répertoire. Il existe plusieurs façons d'accomplir cette tâche. Dans ce didacticiel, vous ajoutez l'utilisateur `ec2-user` au groupe `apache` pour donner au groupe `apache` la propriété du répertoire `/var/www` et attribuer les autorisations d'écriture au groupe.

Pour définir les autorisations sur les fichiers

1. Ajoutez votre utilisateur (dans ce cas, `ec2-user`) au groupe `apache`.

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

2. Déconnectez-vous, puis reconnectez-vous pour sélectionner le nouveau groupe, puis vérifiez votre adhésion.

   a. Déconnectez-vous (utilisez la commande exit ou fermez la fenêtre de terminal) :

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

   b. Pour vérifier votre adhésion au groupe `apache`, reconnectez-vous à votre instance, puis exécutez la commande suivante :

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

3. Remplacez la propriété de groupe de `/var/www` et son contenu par le groupe `apache`.

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

4. Pour ajouter des autorisations d'écriture de groupe et définir l'ID de groupe pour les futurs sous-répertoires, modifiez les autorisations sur les répertoires de `/var/www` et ses sous-répertoires.

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

5. Pour ajouter des autorisations d'écriture de groupe, modifiez de façon récursive les autorisations sur les fichiers de `/var/www` et ses sous-répertoires :

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

Maintenant, `ec2-user` (et tous les futurs membres du groupe `apache`) peut ajouter, supprimer et modifier les fichiers à la racine du document Apache. Vous pouvez ainsi ajouter du contenu, tel qu'un site Web statique ou une application PHP.

Pour sécuriser votre serveur web (facultatif)

Un serveur web exécutant le protocole HTTP ne fournit aucune sécurité de transport pour les données qu'il envoie ou reçoit. Lorsque vous vous connectez à un serveur HTTP à l'aide d'un navigateur Web, les informations URLs que vous visitez, le contenu des pages Web que vous

recevez et le contenu (y compris les mots de passe) de tous les formulaires HTML que vous soumettez sont visibles par les espions partout sur le réseau. Les bonnes pratiques en matière de sécurisation de votre serveur web consistent à installer la prise en charge HTTPS (HTTP Secure), qui protège vos données grâce au chiffrement SSL/TLS.

Pour plus d'informations sur l'activation de HTTPS sur votre serveur, consultez Tutoriel : Configuration SSL/TLS sur AL2.

Étape 2 : Tester votre serveur LAMP

Si votre serveur est installé et en cours d'exécution, et que vos autorisations sur les fichiers sont correctement définies, votre compte `ec2-user` doit pouvoir créer un fichier PHP simple dans le répertoire `/var/www/html` qui est disponible à partir d'Internet.

Pour tester votre serveur LAMP

1. Créez un fichier PHP à la racine du document Apache.

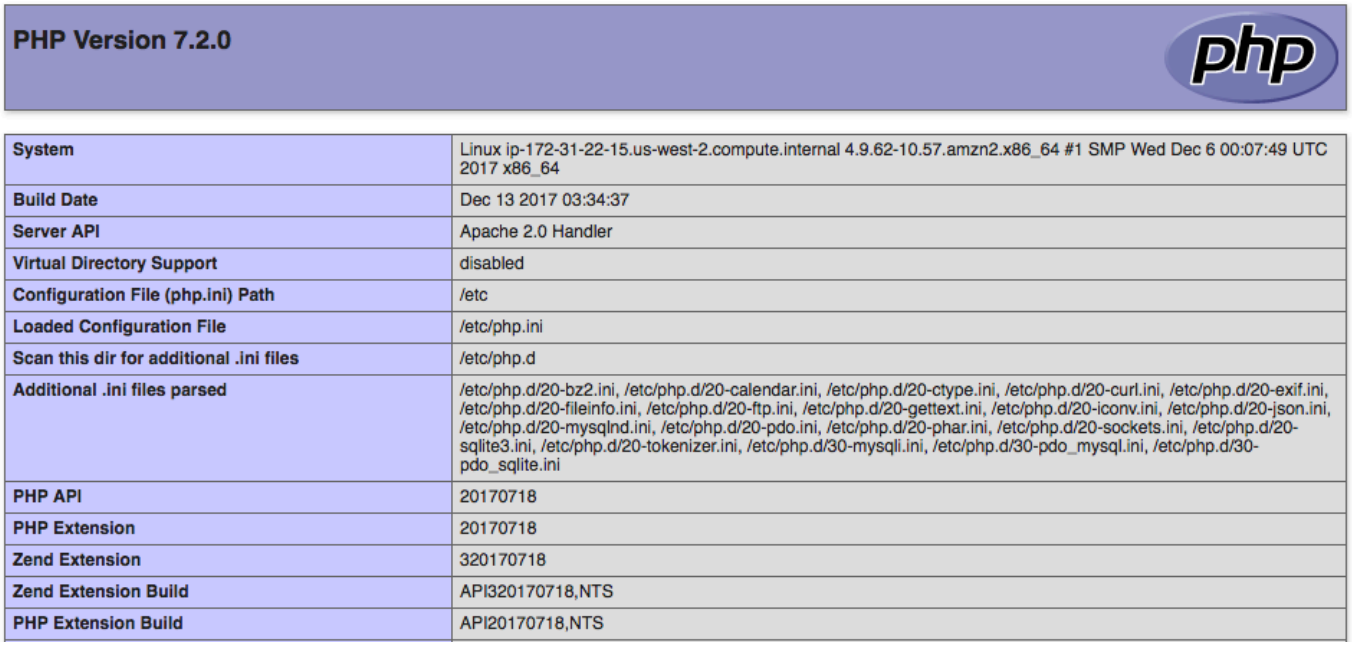
   ```
   [ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
   ```

   Si l'erreur « Permission denied » s'affiche lorsque vous essayez d'exécuter cette commande, essayez de vous déconnecter et de vous reconnecter pour récupérer les autorisations d'un groupe que vous avez configurées dans Pour définir les autorisations sur les fichiers.

2. Dans un navigateur web, saisissez l'URL du fichier que vous venez de créer. Cette URL est l'adresse DNS publique de votre instance suivie par une barre oblique et le nom du fichier. Exemples :

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

   Vous devriez voir la page d'informations PHP:



PHP Version 7.2.0

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

Si vous ne voyez pas cette page, vérifiez que le fichier `/var/www/html/phpinfo.php` a été créé correctement à l'étape précédente. Vous pouvez également vérifier que les packages requis ont été installés avec la commande suivante.

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

Si l'un des packages requis n'est pas présent dans votre sortie, installez-les avec la commande sudo yum install ***package***. Vérifiez également que les référentiels supplémentaires `php7.2` et `lamp-mariadb10.2-php7.2` sont activés dans la sortie de la commande amazon-linux-extras.

3. Supprimez le fichier `phpinfo.php`. Même si ces informations peuvent vous être utiles, elles ne doivent pas être diffusées sur Internet pour des raisons de sécurité.

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

Vous devriez maintenant avoir un serveur web LAMP entièrement fonctionnel. Si vous ajoutez un contenu à la racine du document Apache à l'emplacement `/var/www/html`, vous devez pouvoir voir ce contenu à l'adresse du DNS public de votre instance.

Étape 3 : Sécuriser le serveur de base de données

L'installation par défaut du serveur MariaDB possède plusieurs fonctions qui sont parfaites pour les tests et le développement, mais elles devraient être désactivées ou supprimées des serveurs

de production. La commande mysql_secure_installation vous guide à travers le processus de paramétrage d'un mot de passe racine et de suppression des fonctions non sécurisées de votre installation. Même si vous ne comptez pas utiliser le serveur MariaDB, nous vous recommandons de suivre cette procédure.

Pour sécuriser le serveur MariaDB

1. Démarrez le serveur MariaDB.

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

2. Exécutez mysql_secure_installation.

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

   a. A l'invite, saisissez un mot de passe pour le compte racine.

      i. Saisissez le mot de passe racine actuel. Par défaut, le compte racine n'a pas de mot de passe défini. Appuyez sur Entrée.

      ii. Tapez **Y** pour définir un mot de passe et saisissez deux fois un mot de passe sécurisé. Pour plus d'informations sur la création d'un mot de passe sécurisé, consultez https://identitysafe.norton.com/password-generator/. Assurez-vous de stocker ce mot de passe en lieu sûr.

      La mesure la plus simple pour sécuriser votre base de données consiste à définir un mot de passe racine pour MariaDB. Lorsque vous concevez ou installez une application reposant sur une base de données, vous devez généralement créer un utilisateur de services de base de données pour cette application et éviter d'utiliser le compte racine, sauf pour administrer la base de données.

   b. Tapez **Y** pour supprimer les comptes d'utilisateur anonymes.

   c. Tapez **Y** pour désactiver la connexion racine à distance.

   d. Tapez **Y** pour supprimer la base de données de test.

   e. Tapez **Y** pour recharger les tableaux de privilèges et enregistrer vos changements.

3. (Facultatif) Si vous ne comptez pas utiliser le serveur MariaDB tout de suite, arrêtez-le. Vous pouvez le redémarrer lorsque vous en avez de nouveau besoin.

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

4. (Facultatif) Si vous voulez que le serveur MariaDB soit lancé à chaque démarrage, saisissez la commande suivante.

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

Étape 4 : (Facultatif) Installation phpMyAdmin

phpMyAdminest un outil de gestion de base de données basé sur le Web que vous pouvez utiliser pour afficher et modifier les bases de données MySQL de votre EC2 instance. Suivez les étapes ci-dessous pour installer et configurer `phpMyAdmin` sur votre instance Amazon Linux.

> **Important**
>
> Nous vous déconseillons de l'utiliser `phpMyAdmin` pour accéder à un serveur LAMP sauf si vous l'avez activé SSL/TLS dans Apache ; sinon, votre mot de passe d'administrateur de base de données et d'autres données ne seront pas transmis de manière sécurisée sur Internet. Pour connaître les recommandations de sécurité des développeurs, consultez la section Sécurisation de votre phpMyAdmin installation. Pour obtenir des informations générales sur la sécurisation d'un serveur Web sur une EC2 instance, consultezTutoriel : Configuration SSL/TLS sur AL2.

Pour installer phpMyAdmin

1. Installez les dépendances obligatoires.

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

2. Redémarrez Apache.

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

3. Redémarrez `php-fpm`.

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

4. Accédez à la racine du document Apache sur `/var/www/html`.

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

5. Sélectionnez un package source pour la dernière phpMyAdmin version sur https://www.phpmyadmin.net/downloads. Pour télécharger le fichier directement sur votre instance, copiez le lien et collez-le dans une commande wget, comme dans cet exemple :

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

6. Créez un dossier phpMyAdmin et extrayez le package dans celui-ci avec la commande suivante.

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

7. Supprimez l'*phpMyAdmin-latest-all-languages.tar.gz*archive tar.

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

8. (Facultatif) Si le serveur MySQL n'est pas en cours d'exécution, démarrez-le maintenant.

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

9. Dans un navigateur Web, saisissez l'URL de votre phpMyAdmin installation. Cette URL est l'adresse DNS publique (ou l'adresse IP publique) de votre instance suivie par une barre oblique et le nom du fichier de votre répertoire d'installation. Par exemple :

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

Vous devriez voir la page phpMyAdmin de connexion :

10. Connectez-vous à votre phpMyAdmin installation avec le nom d'`root`utilisateur et le mot de passe root MySQL que vous avez créés précédemment.

    Votre installation doit être configurée avant que vous la mettiez en service. Nous vous suggérons de commencer par créer manuellement le fichier de configuration, comme suit :

    a. Pour commencer avec un fichier de configuration minimal, utilisez votre éditeur de texte favori pour créer un nouveau fichier, puis copiez le contenu de `config.sample.inc.php` dans celui-ci.

    b. Enregistrez le fichier `config.inc.php` dans le phpMyAdmin répertoire qui le contient`index.php`.

    c. Reportez-vous aux instructions après la création du fichier dans la section Utilisation du script d' phpMyAdmin installation des instructions d'installation pour toute configuration supplémentaire.

Pour plus d'informations sur l'utilisation phpMyAdmin, consultez le guide de phpMyAdmin l'utilisateur.

Dépannage

Cette section propose des suggestions pour résoudre les problèmes courants que vous pouvez rencontrer lors de la configuration d'un nouveau serveur LAMP.

Je ne parviens pas à me connecter à mon serveur à l'aide d'un navigateur Web.

Effectuez les vérifications suivantes pour voir si votre serveur web Apache est en cours d'exécution et accessible.

- Le serveur web est-il en cours d'exécution ?

  Vous pouvez vérifier que httpd est activé en exécutant la commande suivante :

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

  Si le processus httpd n'est pas en cours d'exécution, répétez les étapes décrites dans Pour préparer le serveur LAMP.
- Le pare-feu est-il configuré correctement ?

  Vérifiez que le groupe de sécurité de l'instance contient une règle autorisant le trafic HTTP sur le port 80. Pour plus d'informations, voir Ajouter des règles au groupe de sécurité.

Je ne parviens pas à me connecter à mon serveur en utilisant HTTPS

Effectuez les vérifications suivantes pour voir si votre serveur Web Apache est configuré pour prendre en charge HTTPS.

- Le serveur Web est-il correctement configuré ?

  Après avoir installé Apache, le serveur est configuré pour le trafic HTTP. Pour prendre en charge HTTPS, activez TLS sur le serveur et installez un certificat SSL. Pour plus d'informations, veuillez consulter Tutoriel : Configuration SSL/TLS sur AL2.
- Le pare-feu est-il configuré correctement ?

Vérifiez que le groupe de sécurité de l'instance contient une règle autorisant le trafic HTTPS sur le port 443. Pour plus d'informations, voir Ajouter des règles à un groupe de sécurité.

Rubriques en relation

Pour plus d'informations sur le transfert de fichiers vers votre instance ou l'installation d'un WordPress blog sur votre serveur Web, consultez la documentation suivante :

- Transférez des fichiers vers votre instance Linux à l'aide deWinSCP.
- Transférez des fichiers vers des instances Linux à l'aide d'un SCP client.
- Tutoriel : héberger un WordPress blog sur AL2

Pour plus d'informations sur les commandes et le logiciel utilisés dans ce tutoriel, consultez les pages web suivantes :

- Serveur Web Apache : http://httpd.apache.org/
- Serveur de base de données MariaDB : https://mariadb.org/
- Langage de programmation PHP : http://php.net/
- La `chmod` commande : https://en.wikipedia. org/wiki/Chmod
- La `chown` commande : https://en.wikipedia. org/wiki/Chown

Pour plus d'informations sur l'enregistrement d'un nom de domaine pour votre serveur web ou le transfert d'un nom de domaine existant vers cet hôte, consultez Création et migration de domaines et de sous-domaines vers Amazon Route 53 dans le Amazon Route 53 Manuel du développeur.

Tutoriel : Configuration SSL/TLS sur AL2

Secure Sockets Layer/Transport Layer Security (SSL/TLS) creates an encrypted channel between a web server and web client that protects data in transit from being eavesdropped on. This tutorial explains how to add support manually for SSL/TLSsur une EC2 instance avec AL2 un serveur Web Apache). Ce tutoriel suppose que vous n'utilisez pas d'équilibreur de charge. Si vous utilisez Elastic Load Balancing, vous pouvez choisir de configurer le déchargement SSL sur l'équilibreur de charge, en utilisant un certificat à partir de AWS Certificate Manager.

Pour des raisons historiques, le chiffrement web est communément appelé SSL. Alors que les navigateurs web prennent toujours en charge SSL, son protocole successeur TLS est moins

vulnérable en cas d'attaque. AL2 désactive la prise en charge côté serveur pour toutes les versions SSL par défaut. Les organismes de normalisation de la sécurité considèrent que TLS 1.0 n'est pas sûr. TLS 1.0 et TLS 1.1 sont devenus officiellement obsolètes en mars 2021. Ce tutoriel contient des conseils pour l'activation de TLS 1.2 exclusivement. Le protocole TLS 1.3 a été finalisé en 2018 et est disponible AL2 tant que la bibliothèque TLS sous-jacente (OpenSSL dans ce didacticiel) est prise en charge et activée. Les clients doivent prendre en charge le protocole TLS 1.2 ou une version ultérieure d'ici le 28 juin 2023. Pour plus d'informations sur les normes de chiffrement mises à jour, consultez RFC 7568 et RFC 8446.

Ce tutoriel fait référence au chiffrement Web moderne simplement comme TLS.

Important

Ces procédures sont destinées à être utilisées avec AL2. Nous partons également du principe que vous commencez avec une nouvelle EC2 instance Amazon. Si vous essayez de configurer une EC2 instance exécutant une distribution différente ou une instance exécutant une ancienne version de AL2, certaines procédures de ce didacticiel risquent de ne pas fonctionner. Pour Ubuntu, consultez la documentation de la communauté suivante : Open SSL on Ubuntu (Ouvrir SSL sur Ubuntu). Pour Red Hat Enterprise Linux, consultez les informations suivantes :Setting up the Apache HTTP Web Server (Configuration du serveur web HTTP Apache). Pour les autres distributions, consultez leur documentation spécifique.

Note

Vous pouvez également utiliser AWS Certificate Manager (ACM) for AWS Nitro enclaves, une application d'enclave qui vous permet d'utiliser des SSL/TLS certificats publics et privés avec vos applications Web et vos serveurs exécutés sur des EC2 instances Amazon avec Nitro Enclaves. AWS Nitro Enclaves est une EC2 fonctionnalité d'Amazon qui permet de créer des environnements informatiques isolés afin de protéger et de traiter en toute sécurité les données hautement sensibles, telles que les SSL/TLS certificats et les clés privées.
ACM for Nitro Enclaves fonctionne avec nginx exécuté sur votre instance EC2 Amazon Linux pour créer des clés privées, distribuer des certificats et des clés privées et gérer les renouvellements de certificats.
Pour utiliser ACM for Nitro Enclaves, vous devez utiliser une instance Linux compatible avec les enclaves.

Pour plus d'informations, consultez Qu'est-ce que AWS Nitro Enclaves ? et AWS Certificate Manager pour Nitro Enclaves dans le guide de l'utilisateur de AWS Nitro Enclaves.

Table des matières

Conditions préalables

Avant de commencer ce tutoriel, suivez les étapes suivantes :

- Lancez une AL2 instance basée sur Amazon EBS. Pour plus d'informations, consultez Lancer une instance dans le guide de EC2 l'utilisateur Amazon.
- Configurez vos groupes de sécurité afin que votre instance puisse accepter des connexions sur les ports TCP suivants :
  - SSH (port 22)
  - HTTP (port 80)
  - HTTPS (port 443)

  Pour plus d'informations, consultez la section Règles relatives aux groupes de sécurité dans le guide de EC2 l'utilisateur Amazon.
- Installez le serveur Web Apache. Pour step-by-step obtenir des instructions, voir Tutoriel : Installation d'un serveur Web LAMP sur AL2. Seuls le package httpd et ses dépendances sont nécessaires. Par conséquent, vous pouvez ignorer les instructions impliquant PHP et MariaDB.
- Pour identifier et authentifier les sites web, l'infrastructure à clés publiques (PKI) TLS repose sur le système de noms de domaine (DNS). Pour utiliser votre EC2 instance pour héberger un site Web public, vous devez enregistrer un nom de domaine pour votre serveur Web ou transférer un nom de domaine existant vers votre EC2 hôte Amazon. Plusieurs services d'enregistrement de domaines tiers et d'hébergement DNS sont disponibles pour cela, ou vous pouvez utiliser Amazon Route 53.

Étape 1 : Activer TLS sur le serveur

Option : Effectuer ce tutoriel en utilisant Automation

Pour terminer ce didacticiel en utilisant AWS Systems Manager Automation au lieu des tâches suivantes, exécutez le document d'automatisation.

Cette procédure vous guide dans le processus de configuration du protocole TLS AL2 avec un certificat numérique autosigné.

> **Note**
>
> Un certificat auto-signé est acceptable dans un environnement de test, mais pas pour les environnements de production. Si vous exposez votre certificat auto-signé sur Internet, les visiteurs de votre site verront s'afficher des messages d'avertissement de sécurité.

Pour activer TLS sur un serveur

1. Connectez-vous à votre instance et confirmez qu'Apache est en cours d'exécution.

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

   Si la valeur renvoyée n'est pas « activé », démarrez Apache et configurez-le pour qu'il démarre à chaque amorçage du système.

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

2. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance. Ce processus peut prendre quelques minutes, mais il est important pour vous assurer que vous disposez des dernières mises à jour de sécurité et des nouveaux correctifs de bogues.

   > **Note**
   >
   > L'option `-y` installe les mises à jour sans demander de confirmation. Si vous souhaitez examiner les mises à jour avant l'installation, vous pouvez omettre cette option.

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

3. Maintenant que votre instance est à jour, ajoutez la prise en charge de TLS en installant le module Apache `mod_ssl`.

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

Votre instance dispose désormais des fichiers suivants que vous utilisez pour configurer votre serveur sécurisé et créer un certificat pour les tests :

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

  Le fichier de configuration de mod_ssl. Il contient des directives indiquant à Apache où trouver les clés et les certificats de chiffrement, les versions de protocoles TLS à autoriser et les algorithmes de chiffrement à accepter.

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

  Script pour générer un certificat X.509 auto-signé et une clé privée pour votre hôte serveur. Ce certificat est utile pour vérifier qu'Apache est correctement paramétré pour utiliser TLS. Comme il n'offre aucune preuve d'identité, il ne doit pas être utilisé en production. S'il est utilisé en production, il déclenche des avertissements dans les navigateurs web.

4. Exécutez le script pour générer un certificat factice auto-signé et une clé pour les tests.

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

Cela génère un nouveau fichier `localhost.crt` dans le répertoire `/etc/pki/tls/certs/`. Le nom de fichier spécifié correspond au nom par défaut attribué dans la directive SSLCertificateFile dans `/etc/httpd/conf.d/ssl.conf`.

Ce fichier contient un certificat auto-signé et la clé privée du certificat. Apache exige que le certificat et la clé soient au format PEM qui est constitué de caractères ASCII codés en Base64, encadrés par des lignes « BEGIN » et « END », comme dans l'exemple abrégé ci-après.

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

Les noms et extensions de fichiers sont fournis à titre indicatif et n'ont aucun effet sur la fonction. Par exemple, vous pouvez appeler un certificat `cert.crt`, `cert.pem`, ou tout autre nom de fichier dans la mesure où la directive associée dans le fichier `ssl.conf` utilise le même nom.

> **Note**
>
> Lorsque vous remplacez les fichiers TLS par défaut par vos propres fichiers personnalisés, veillez à ce qu'ils soient au format PEM.

5. Ouvrez le fichier `/etc/httpd/conf.d/ssl.conf` en utilisant votre éditeur préféré (comme vim ou nano) en tant qu'utilisateur root et mettez en commentaire la ligne suivante, car le certificat fictif signé automatiquement contient aussi la clé. Si vous ne le faites pas avant d'exécuter l'étape suivante, le service Apache ne peut pas démarrer.

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

6. Redémarrez Apache.

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

> **Note**
>
> Assurez-vous que le port TCP 443 est accessible sur votre EC2 instance, comme décrit précédemment.

7. Votre serveur web Apache devrait maintenant prendre en charge HTTPS (HTTP sécurisé) sur le port 443. Testez-le en saisissant l'adresse IP ou le nom de domaine complet de votre EC2 instance dans la barre d'URL du navigateur avec le préfixe**`https://`**.

   Étant donné que vous vous connectez à un site avec un certificat d'hôte auto-signé non approuvé, il se peut que votre navigateur affiche une série d'avertissements de sécurité. Ignorez-les et poursuivez sur le site.

   Si la page de test Apache par défaut s'ouvre, cela signifie que vous avez configuré correctement TLS sur votre serveur. Toutes les données transmises entre le navigateur et le serveur sont maintenant chiffrées.

   > **Note**
   >
   > Pour éviter aux visiteurs du site d'avoir des avertissements, vous devez obtenir un certificat signé par une CA qui chiffre mais vous authentifie aussi publiquement comme le propriétaire du site.

Étape 2 : Obtenir un certificat signé par une autorité de certification (CA)

Vous pouvez utiliser le processus suivant pour obtenir un certificat signé par une CA :

- Générez une demande de signature de certificat (CSR) à partir d'une clé privée
- Envoyez la demande de signature de certificat (CSR) à une autorité de certification (CA)
- Obtenez un certificat d'hôte signé
- Configurez Apache pour utiliser le certificat

Le chiffrement d'un certificat X.509 TLS auto-signé est identique à celui d'un certificat signé par une autorité de certification. La différence est sociale, pas mathématique. Une autorité de certification promet, au minimum, de valider la propriété d'un domaine avant de générer un certificat pour un demandeur. Chaque navigateur Web contient une liste des navigateurs auxquels le fournisseur du

navigateur CAs fait confiance pour ce faire. Un certificat X.509 se compose surtout d'une clé publique qui correspond à votre clé de serveur privée et d'une signature de l'autorité de certification qui est cryptographiquement reliée à la clé publique. Lorsqu'un navigateur se connecte à un serveur Web via HTTPS, le serveur présente un certificat permettant au navigateur de vérifier sa liste de sites fiables CAs. Si le signataire est sur la liste ou s'il est accessible via une chaîne de confiance composée d'autres utilisateurs de confiance, le navigateur négocie un canal de données chiffrées rapide avec le serveur et charge la page.

Les certificats coûtent généralement de l'argent à cause travail impliqué dans la validation des requêtes, donc il est intéressant de comparer les prix. Quelques-uns CAs proposent des certificats de base gratuits. Le plus remarquable d'entre eux CAs est le projet Let's Encrypt, qui prend également en charge l'automatisation du processus de création et de renouvellement des certificats. Pour plus d'informations sur l'utilisation d'un certificat Let's Encrypt, veuillez consulter la rubrique Get Certbot.

Si vous prévoyez d'offrir des services de qualité commerciale, AWS Certificate Manager est une bonne option.

La clé est l'élément sous-jacent du certificat d'hôte. Depuis 2019, des groupes gouvernementaux et industriels recommandent l'utilisation d'une taille de clé minimale (module) de 2048 bits pour les clés RSA conçues pour protéger des documents, jusqu'en 2030. La taille du module par défaut générée par OpenSSL AL2 in est de 2048 bits, ce qui convient à une utilisation dans un certificat signé par une autorité de certification. Dans la procédure suivante, étape facultative pour ceux qui souhaitent une clé personnalisée, par exemple, une clé avec un module plus important ou utilisant un algorithme de chiffrement différent.

> **Important**
>
> Ces instructions pour l'acquisition de certificats d'hôte signés par l'autorité de certification (CA) ne fonctionnent pas à moins que vous possédiez un domaine DNS enregistré et hébergé.

Pour obtenir un certificat signé par une CA

1. Connectez-vous à votre instance et accédez à/etc/pki/tls/private/. Il s'agit du répertoire où vous stockez la clé privée du serveur pour TLS. Si vous préférez utiliser une clé d'hôte existante pour générez la CSR, passez à l'étape 3.

2. (Facultatif) Générez une nouvelle clé privée. Voici quelques exemples de configurations de clés. Toutes les clés obtenues fonctionnent avec votre serveur web, mais elles diffèrent dans le degré et le type de sécurité qu'elles mettent en œuvre.

   - Exemple 1 : création d'une clé d'hôte RSA par défaut. Le fichier obtenu, **`custom.key`**, est une clé privée RSA 2048 bits.

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

   - Exemple 2 : création d'une clé RSA plus forte avec un modulus plus grand. Le fichier obtenu, **`custom.key`**, est une clé privée RSA 4096 bits.

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

   - Exemple 3 : création d'une clé RSA chiffrée 4096 bits avec protection par mot de passe. Le fichier obtenu, **`custom.key`**, est une clé privée RSA 4096 bits chiffrée avec le chiffrement AES-128.

     > **Important**
     >
     > Le chiffrement de la clé offre une plus grande sécurité, mais comme une clé chiffrée nécessite un mot de passe, les services qui en dépendent ne peuvent pas démarrer automatiquement. A chaque fois que vous utilisez cette clé, vous devez fournir le mot de passe (« abcde12345 » dans l'exemple précédent) sur une connexion SSH.

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

   - Exemple 4 : création d'une clé avec un chiffrement non RSA. La cryptographie RSA peut être relativement lente en raison de la taille de ses clés publiques, lesquelles sont basées sur le produit de deux grands nombres premiers. Cependant, il est possible de créer des clés pour TLS qui utilisent des chiffrements non RSA. Les clés basées sur les mathématiques des courbes elliptiques sont plus petites et plus rapides en termes de calcul, tout en offrant un niveau de sécurité équivalent.

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

Le résultat est une clé privée 256 bits à courbes elliptiques utilisant prime256v1, une « courbe nommée » que OpenSSL prend en charge. Sa qualité cryptographique est légèrement plus importante qu'une clé RSA 2048 bits, selon NIST.

> **Note**
>
> Tous ne CAs fournissent pas le même niveau de support pour les elliptic-curve-based clés que pour les clés RSA.

Assurez-vous que la propriété et les autorisations de la nouvelle clé privée sont très restrictives (owner=root, group=root, read/write pour le propriétaire uniquement). Les commandes seraient similaires à celles illustrées dans l'exemple suivant.

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

Les commandes ci-avant produisent le résultat suivant.

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

Une fois que vous avez créé et configuré une clé satisfaisante, vous pouvez créer une CSR.

3. Créez une CSR à l'aide de votre clé préférée. L'exemple suivant utilise **`custom.key`**.

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

OpenSSL ouvre une boîte de dialogue et vous invite à compléter les informations affichées dans le tableau ci-dessous. Tous les champs à l'exception de Common Name sont facultatifs pour un certificat d'hôte basique avec validation de domaine.

Nom	Description	Exemple
Nom du pays	Abréviation ISO de deux lettres de votre pays.	US (=Etats-Unis)

Nom	Description	Exemple
Nom de l'état ou de la province	Nom de l'état ou de la province où votre organisation se situe. Ce nom ne peut pas être abrégé.	Washington
Nom de la localité	L'emplacement de votre organisation, comme une ville.	Seattle
Nom de l'organisation	Nom légal complet de votre organisation. N'abrégez pas le nom de votre organisation.	Exemple d'entreprise
Nom de l'unité d'organisation	Informations supplémentaires sur l'organisation, s'il y en a.	Exemple de service
Nom commun	Cette valeur doit correspondre exactement à l'adresse web que les utilisateurs saisiront dans un navigateur, selon vous. Il s'agit généralement d'un nom de domaine avec un nom d'hôte ou un alias préfixé sous la forme **`www.example.com`** . Lors des tests effectués avec un certificat auto-signé et sans résolution DNS, le nom commun peut être composé uniquement du nom d'hôte. CAs proposent également des certificats plus chers qui acceptent des noms génériques tels que. **`*.example.com`**	www.exemple.com
Adresse e-mail	L'adresse e-mail de l'administrateur du serveur.	quelquun@exemple.com

Au final, OpenSSL vous invite à donner un mot de passe de stimulation facultatif. Ce mot de passe s'applique uniquement à la CSR et aux transactions entre vous et votre autorité de certification, donc suivez les recommandations de l'autorité de certification sur cela, l'autre

champ facultatif et le nom de l'entreprise facultatif. Le mot de passe de stimulation de la CSR n'a aucun effet sur le fonctionnement du serveur.

Le fichier obtenu **csr.pem** contient votre clé publique, la signature numérique de votre clé publique et les métadonnées que vous avez saisies.

4. Envoyez la CSR à une autorité de certification. Elle consiste généralement en l'ouverture de votre fichier CSR dans un éditeur de texte et la reproduction du contenu dans un formulaire web. À ce stade, il peut vous être demandé de fournir un ou plusieurs noms alternatifs de sujet (SANs) à placer sur le certificat. Si **www.example.com** est le nom commun, **example.com** serait un bon SAN, et vice versa. Un visiteur de votre site qui saisit l'un de ces noms devrait bénéficier d'une connexion sans erreur. Si votre formulaire Web CA le permet, incluez le nom commun dans la liste des SANs. Certains l' CAs incluent automatiquement.

   Une fois que votre demande a été approuvée, vous recevrez un nouveau certificat d'hôte signé par l'autorité de certification. Il se peut que l'on vous demande également de télécharger un fichier de certificat intermédiaire qui contient des certificats supplémentaires nécessaires pour compléter la chaîne de confiance de l'autorité de certification.

   > **Note**
   >
   > Votre autorité de certification peut vous envoyer des fichiers sous différents formats en fonction des finalités recherchées. Dans ce tutoriel, vous devez utiliser uniquement un fichier de certificat au format PEM, qui comporte habituellement (mais pas toujours) une extension de fichier `.pem` ou `.crt`. Si vous ne savez pas quel fichier utiliser, ouvrez les fichiers dans un éditeur de texte et recherchez celui qui contient un ou plusieurs blocs commençant par la ligne suivante.
   >
   > ```
   > - - - - -BEGIN CERTIFICATE - - - - -
   > ```
   >
   > Le fichier doit également se terminer par la ligne suivante.
   >
   > ```
   > - - - -END CERTIFICATE - - - - -
   > ```
   >
   > Vous pouvez également tester le fichier dans la ligne de commande, comme suit.
   >
   > ```
   > [ec2-user certs]$ openssl x509 -in certificate.crt -text
   > ```

Vérifiez que ces lignes apparaissent dans le fichier. N'utilisez pas de fichiers se terminant par `.p7b`, `.p7c` ou autres extensions similaires.

5. Placez le nouveau certificat signé par une CA et les certificats intermédiaires dans le répertoire `/etc/pki/tls/certs`.

> **Note**
>
> Il existe plusieurs méthodes pour télécharger votre nouveau certificat sur votre EC2 instance, mais la méthode la plus simple et la plus informative consiste à ouvrir un éditeur de texte (par exemple, vi, nano ou bloc-notes) à la fois sur votre ordinateur local et sur votre instance, puis à copier-coller le contenu du fichier entre eux. Vous devez disposer des autorisations root [sudo] pour effectuer ces opérations sur l' EC2instance. Vous voyez ainsi immédiatement s'il existe des problèmes d'autorisation ou de chemin d'accès. Veillez toutefois à ne pas d'ajouter des lignes supplémentaires lors de la copie du contenu, ou à les modifier de quelque façon.

Depuis le `/etc/pki/tls/certs` répertoire, vérifiez que les paramètres de propriété, de groupe et d'autorisation du fichier correspondent aux AL2 valeurs par défaut très restrictives (owner=root, group=root, pour le propriétaire uniquement). read/write L'exemple suivant illustre les commandes à utiliser.

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

Ces commandes devraient générer le résultat suivant.

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

Les autorisations pour le fichier de certificat intermédiaire sont moins contraignantes (propriétaire=racine, groupe=racine, le propriétaire peut écrire, le groupe peut lire, tout le monde peut lire). L'exemple suivant illustre les commandes à utiliser.

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

```
[ec2-user certs]$ ls -al intermediate.crt
```

Ces commandes devraient générer le résultat suivant.

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

6. Placez la clé privée que vous avez utilisée pour créer la CSR dans le répertoire `/etc/pki/tls/private/`.

> **Note**
>
> Il existe plusieurs méthodes pour télécharger votre clé personnalisée sur votre EC2 instance, mais la méthode la plus simple et la plus informative consiste à ouvrir un éditeur de texte (par exemple, vi, nano ou bloc-notes) à la fois sur votre ordinateur local et sur votre instance, puis à copier-coller le contenu du fichier entre eux. Vous devez disposer des autorisations root [sudo] pour effectuer ces opérations sur l' EC2instance. Vous voyez ainsi immédiatement s'il existe des problèmes d'autorisation ou de chemin d'accès. Veillez toutefois à ne pas d'ajouter des lignes supplémentaires lors de la copie du contenu, ou à les modifier de quelque façon.

Depuis le `/etc/pki/tls/private` répertoire, utilisez les commandes suivantes pour vérifier que les paramètres de propriété, de groupe et d'autorisation du fichier correspondent aux AL2 valeurs par défaut très restrictives (owner=root, group=root, pour le propriétaire uniquement). read/write

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

Ces commandes devraient générer le résultat suivant.

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

7. Modifiez `/etc/httpd/conf.d/ssl.conf` pour refléter les nouveaux fichiers de certificat et de clé.

a. Fournissez le chemin et le nom de fichier du certificat d'hôte signé par une CA dans la directive `SSLCertificateFile` d'Apache :

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

b. Si vous avez reçu un fichier de certificat intermédiaire (`intermediate.crt` dans cet exemple), indiquez son nom correct de chemin et de fichier à l'aide de la directive `SSLCACertificateFile` d'Apache :

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

> **Note**
>
> Certains CAs combinent le certificat hôte et les certificats intermédiaires dans un seul fichier, ce qui rend la `SSLCACertificateFile` directive inutile. Consultez les instructions fournies par votre autorité de certification.

c. Fournissez le chemin et le nom de fichier de la clé privée (`custom.key` dans cet exemple) dans la directive `SSLCertificateKeyFile` d'Apache :

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

8. Enregistrez `/etc/httpd/conf.d/ssl.conf` et redémarrez Apache.

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

9. Testez votre serveur en saisissant votre nom de domaine dans la barre d'URL de navigateur avec le préfixe `https://`. Votre navigateur doit charger la page de test via HTTPS sans générer d'erreurs.

Étape 3 : Tester et renforcer la configuration de sécurité

Une fois que votre TLS est opérationnel et exposé au public, vous devriez tester son niveau de sécurité. Il est facile de le faire avec des services en ligne comme Qualys SSL Labs qui effectue une analyse gratuite et complète de votre configuration de sécurité. En fonction des résultats, vous pouvez décider de renforcer la configuration de sécurité par défaut en contrôlant les protocoles que

vous acceptez, les chiffrements que vous préférez et que vous excluez. Pour plus d'informations, consultez comment Qualys formule ses scores.

> **Important**
>
> Le test concret est essentiel pour la sécurité de votre serveur. Les petites erreurs de configuration peuvent entraîner des failles de sécurité et des pertes de données. Comme les pratiques de sécurité recommandées changent constamment en réponse à la recherche et aux menaces émergentes, des audits de sécurité périodiques sont essentiels pour la bonne administration du serveur.

Sur le site Qualys SSL Labs, saisissez le nom de domaine complet de votre serveur dans le formulaire **`www.example.com`**. Après environ deux minutes, vous recevrez une note (de A à F) pour votre site et une analyse détaillée des résultats. Le tableau suivant résume le rapport pour un domaine dont les paramètres sont identiques à ceux de la configuration Apache par défaut et avec un certificat Certbot par défaut. AL2

Score général	B
Certificat	100 %
Support du protocole	95 %
Échange de clés	70 %
Force du chiffrement	90 %

Même si l'aperçu montre que la configuration est principalement sûre, le rapport détaillé indique plusieurs problèmes potentiels, répertoriés ici dans l'ordre de gravité :

✗ Le RC4 chiffrement est compatible avec certains anciens navigateurs. Un chiffrement est le noyau mathématique d'un algorithme de chiffrement. RC4, un algorithme de chiffrement rapide utilisé pour chiffrer les flux de données TLS, est connu pour présenter plusieurs faiblesses graves. À moins que vous ayez une très bonne raison de prendre en charge des navigateurs existants, vous devez désactiver cette option.

✗ Les anciennes versions de TLS sont prises en charge. La configuration prend en charge TLS 1.0 (déjà obsolète) et TLS 1.1 (bientôt obsolète). Seul TLS 1.2 est recommandé depuis 2018.

✗ La confidentialité persistante n'est pas entièrement prise en charge. La confidentialité persistante est une fonction des algorithmes qui chiffrent à l'aide de clés de session temporaires (éphémères) issues de la clé privée. Ceci signifie en pratique que les pirates informatiques ne peuvent pas déchiffrer les données HTTPS même s'ils possèdent la clé privée à long terme d'un serveur web.

Pour corriger et prévenir les erreurs de configuration TLS

1. Ouvrez le fichier de configuration `/etc/httpd/conf.d/ssl.conf` dans un éditeur de texte et mettez en commentaire la ligne suivante en saisissant « # » au début de la ligne.

   ```
   #SSLProtocol all -SSLv3
   ```

2. Ajoutez la directive suivante :

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

   Cette directive désactive explicitement les versions SSL 2 et 3, ainsi que les versions TLS 1.0 et 1.1. Le serveur refuse désormais d'accepter les connexions chiffrées avec des clients utilisant tout sauf TLS 1.2. La formulation des commentaires dans la directive indique plus clairement, à un lecteur humain, ce pour quoi le serveur est configuré.

   > **Note**
   >
   > La désactivation des versions TLS 1.0 et 1.1 de cette manière empêche un faible pourcentage de navigateurs web obsolètes d'accéder à votre site.

Pour modifier la liste des chiffrements autorisés

1. Dans le fichier de configuration `/etc/httpd/conf.d/ssl.conf`, recherchez la section avec la directive **`SSLCipherSuite`** et mettez en commentaire la ligne existante en saisissant « # » au début de la ligne.

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

2. Spécifiez explicitement des suites de chiffrement et un ordre de chiffrement qui donnent la priorité à la confidentialité persistante et évitent les chiffrements peu sûrs. La directive `SSLCipherSuite` utilisée ici est basée sur la sortie du Mozilla SSL Configuration Generator, qui adapte une configuration TLS au logiciel spécifique s'exécutant sur votre serveur. Déterminez d'abord vos versions d'Apache et OpenSSL en utilisant la sortie des commandes suivantes.

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

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

Par exemple, si l'information renvoyée est Apache 2.4.34 et OpenSSL 1.0.2, nous saisissons cela dans le générateur. Si vous choisissez le modèle de compatibilité « moderne », il crée une directive `SSLCipherSuite` qui applique la sécurité de façon stricte, tout en étant compatible avec la plupart des navigateurs. Si votre logiciel ne prend pas en charge la configuration moderne, vous pouvez mettre à jour le logiciel ou choisir la configuration « intermédiaire ».

```
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
```

Les chiffrements sélectionnés contiennent ECDHE (une abréviation pour Elliptic Curve Diffie-Hellman Ephemeral) dans leur nom. Le terme ephemeral indique la confidentialité persistante. En tant que sous-produit, ces chiffrements ne sont pas compatibles. RC4

Nous vous recommandons d'utiliser une liste explicite de chiffrements au lieu de compter sur les valeurs par défaut ou les directives succinctes dont le contenu n'est pas visible.

Copiez la directive générée dans `/etc/httpd/conf.d/ssl.conf`.

> **Note**
>
> Même si la directive est affichée ici sur plusieurs lignes afin d'être plus lisible, elle doit être sur une seule ligne lorsqu'elle est copiée dans `/etc/httpd/conf.d/ssl.conf` avec un point (pas d'espace) entre les noms des chiffrements.

3. En dernier lieu, supprimez la mise en commentaire de la ligne suivante en retirant le « # » au début de la ligne.

   ```
   #SSLHonorCipherOrder on
   ```

   Cette directive force le serveur à préférer les chiffrements de niveau élevé notamment (dans ce cas) ceux qui prennent en charge la confidentialité persistante. Avec cette directive activée, le serveur essaie d'établir une connexion très sécurisée avant d'avoir recours aux chiffrements autorisés dotés d'une sécurité moindre.

Après avoir terminé ces deux procédures, enregistrez les modifications dans `/etc/httpd/conf.d/ssl.conf` et redémarrez Apache.

Si vous testez à nouveau le domaine sur Qualys SSL Labs, vous devriez constater que la RC4 vulnérabilité et les autres avertissements ont disparu et que le résumé ressemble à ce qui suit.

Score général	A
Certificat	100 %
Support du protocole	100 %
Échange de clés	90 %
Force du chiffrement	90 %

Chaque mise à jour d'OpenSSL présente de nouveaux chiffrements et supprime le support des anciens. Conservez votre EC2 AL2 instance up-to-date, surveillez les annonces de sécurité d'OpenSSL et soyez attentif aux informations faisant état de nouveaux exploits de sécurité dans la presse technique.

Dépannage

- Mon serveur Web Apache ne démarre pas si je ne fournis pas un mot de passe

  Il s'agit du comportement attendu si vous avez installé une clé de serveur privée chiffrée et protégée par mot de passe.

Vous pouvez supprimer l'obligation de chiffrement et de mot de passe de la clé. En supposant qu'une clé RSA privée chiffrée est appelée `custom.key` dans le répertoire par défaut et que son mot de passe est le cas**abcde12345**, exécutez les commandes suivantes sur votre EC2 instance pour générer une version non chiffrée de la clé.

```
[ec2-user ~]$ cd /etc/pki/tls/private/
[ec2-user private]$ sudo cp custom.key custom.key.bak
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out
 custom.key.nocrypt
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key
[ec2-user private]$ sudo chown root:root custom.key
[ec2-user private]$ sudo chmod 600 custom.key
[ec2-user private]$ sudo systemctl restart httpd
```

Apache devrait maintenant démarrer sans vous demander de fournir un mot de passe.

- J'obtiens des erreurs lorsque j'exécute sudo yum install -y mod_ssl.

  Lorsque vous installez les packages requis pour SSL, vous pouvez voir des erreurs similaires à ce qui suit.

  ```
  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
  ```

  Cela signifie généralement que votre EC2 instance n'est pas en cours d'exécution AL2. Ce didacticiel prend uniquement en charge les instances récemment créées à partir d'une AMI AL2 officielle.

Tutoriel : héberger un WordPress blog sur AL2

Les procédures suivantes vous aideront à installer, configurer et sécuriser un WordPress blog sur votre AL2 instance. Ce didacticiel est une bonne introduction à l'utilisation d'Amazon EC2 dans la mesure où vous avez le contrôle total d'un serveur Web qui héberge votre WordPress blog, ce qui n'est pas typique d'un service d'hébergement traditionnel.

Vous êtes responsable de la mise à jour des packages logiciels et de la gestion des correctifs de sécurité pour votre serveur. Pour une WordPress installation plus automatisée qui ne nécessite pas d'interaction directe avec la configuration du serveur Web, le CloudFormation service fournit un WordPress modèle qui peut également vous aider à démarrer rapidement. Pour de plus amples

informations, veuillez consulter Démarrez dans le AWS CloudFormation Guide de l'utilisateur.
Si vous avez besoin d'une solution de haute disponibilité avec une base de données découplée, consultez la section Déploiement d'un WordPress site Web à haute disponibilité dans le guide du développeur.AWS Elastic Beanstalk

> **Important**
>
> Ces procédures sont destinées à être utilisées avec AL2. Pour obtenir plus d'informations sur d'autres distributions, consultez leur documentation spécifique. Plusieurs étapes de ce tutoriel ne fonctionnent pas sur des instances Ubuntu. Pour obtenir de l'aide concernant l'installation WordPress sur une instance Ubuntu, consultez WordPressla documentation Ubuntu. Vous pouvez également l'utiliser CodeDeploypour accomplir cette tâche sur les systèmes Amazon Linux, macOS ou Unix.

Rubriques

Conditions préalables

Ce didacticiel part du principe que vous avez lancé une AL2 instance avec un serveur Web fonctionnel compatible avec PHP et une base de données (MySQL ou MariaDB) en suivant toutes les étapes décrites. Tutoriel : Installation d'un serveur LAMP sur AL2 Ce tutoriel propose aussi des étapes pour la configuration d'un groupe de sécurité afin de permettre le trafic HTTP et HTTPS ainsi que plusieurs étapes afin de vous assurer que les autorisations sur les fichiers sont définies correctement pour votre serveur web. Pour plus d'informations sur l'ajout de règles à votre groupe de sécurité, voir Ajouter des règles à un groupe de sécurité.

Nous vous recommandons vivement d'associer une adresse IP élastique (EIP) à l'instance que vous utilisez pour héberger un WordPress blog. Cela évite à l'adresse DNS publique de votre instance de changer et de détériorer votre installation. Si vous possédez un nom de domaine et que vous voulez l'utiliser pour votre blog, vous pouvez mettre à jour l'enregistrement DNS pour que le nom de domaine pointe vers votre EIP (afin d'obtenir de l'aide à ce sujet, veuillez contacter votre serveur d'inscriptions des noms de domaine). Vous pouvez avoir une EIP associée à une instance en cours

d'exécution sans coût aucun. Pour plus d'informations, consultez la section Adresses IP élastiques dans le guide de EC2 l'utilisateur Amazon.

Si vous n'avez pas encore de nom de domaine pour votre blog, vous pouvez enregistrer un nom de domaine avec Route 53 et associer l'adresse EIP de votre instance à votre nom de domaine. Pour de plus amples informations, veuillez consulter Inscription de noms de domaines à l'aide d'Amazon Route 53 dans le manuel Amazon Route 53 Manuel du développeur.

Installer WordPress

Option : Effectuer ce tutoriel en utilisant Automation

Pour terminer ce didacticiel en utilisant AWS Systems Manager Automation au lieu des tâches suivantes, exécutez le document d'automatisation.

Connectez-vous à votre instance et téléchargez le package WordPress d'installation.

Pour télécharger et décompresser le package WordPress d'installation

1. Téléchargez le dernier package WordPress d'installation à l'aide de la wget commande. La commande suivante devrait toujours télécharger la dernière version.

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

2. Décompressez et désarchivez le package d'installation. Le dossier d'installation est décompressé dans un dossier appelé `wordpress`.

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

Pour créer un utilisateur de base de données et une base de données pour votre WordPress installation

Votre WordPress installation doit stocker des informations, telles que les articles de blog et les commentaires des utilisateurs, dans une base de données. Cette procédure vous aide à créer la base de données de votre blog et un utilisateur qui est autorisé à lire et à enregistrer des informations dans cette dernière.

1. Démarrez le serveur de base de données.

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

2. Connectez-vous au serveur de base de données en tant qu'utilisateur `root`. Saisissez votre mot de passe `root` de base de données lorsque vous y êtes invité. Il peut être différent du mot de passe `root` de votre système ou il peut même être inexistant si vous n'avez pas sécurisé votre serveur de base de données.

   Si vous n'avez pas encore sécurisé votre serveur de base de données, il est important de le faire. Pour plus d'informations, consultez Pour sécuriser le serveur MariaDB (AL2).

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

3. Créez un utilisateur et un mot de passe pour votre base de données MySQL. Votre WordPress installation utilise ces valeurs pour communiquer avec votre base de données MySQL.

   Assurez-vous de créer un mot de passe fiable pour votre utilisateur. N'utilisez pas l'apostrophe (') dans votre mot de passe, car elle détériorera la commande précédente. Ne réutilisez pas un mot de passe existant et assurez-vous de stocker ce mot de passe dans un endroit sûr.

   Saisissez la commande suivante en remplaçant les informations par un nom utilisateur et un mot de passe uniques.

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

4. Créez votre base de données. Donnez à votre base de données un nom descriptif pertinent comme `wordpress-db`.

   > **Note**
   >
   > Les signes de ponctuation autour du nom de la base de données dans la commande ci-dessous sont appelés « accents graves ». La touche « accent grave » (`) est généralement située au-dessus de la touche Tab d'un clavier QWERTY standard. Les « accents graves » ne sont pas toujours nécessaires, mais ils vous permettent d'utiliser des caractères qui sont normalement interdits dans les noms de base de données, comme les traits d'union.

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

5. Accordez des privilèges complets pour votre base de données à l' WordPress utilisateur que vous avez créé précédemment.

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

6. Annulez les privilèges de base de données pour récupérer tous vos changements.

```
FLUSH PRIVILEGES;
```

7. Quittez le client `mysql`.

```
exit
```

Pour créer et modifier le fichier wp-config.php

Le dossier WordPress d'installation contient un exemple de fichier de configuration appelé`wp-config-sample.php`. Dans cette procédure, vous copiez ce fichier avant de le modifier pour respecter votre configuration spécifique.

1. Copiez le fichier `wp-config-sample.php` sur un fichier appelé `wp-config.php`. Cela crée un nouveau fichier de configuration et garde le modèle de fichier original intact comme sauvegarde.

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

2. Modifiez le fichier `wp-config.php` avec votre éditeur de texte préféré (comme nano ou vim) et saisissez les valeurs pour votre installation. Si vous n'avez pas d'éditeur de texte préféré, `nano` convient aux débutants.

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

   a. Trouvez la ligne qui définit `DB_NAME` et remplacez `database_name_here` par le nom de la base de données que vous avez créée à l'Step 4 de la procédure Pour créer un utilisateur de base de données et une base de données pour votre WordPress installation.

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

   b. Trouvez la ligne qui définit `DB_USER` et remplacez `username_here` par l'utilisateur de base de données que vous avez créé à l'Step 3 de la procédure Pour créer un utilisateur de base de données et une base de données pour votre WordPress installation.

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

c. Trouvez la ligne qui définit DB_PASSWORD et remplacez `password_here` par le mot de passe fiable que vous avez créé à l'Step 3 de la procédure Pour créer un utilisateur de base de données et une base de données pour votre WordPress installation.

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

d. Trouvez la section appelée `Authentication Unique Keys and Salts`. Ces SALT valeurs KEY et ces valeurs fournissent une couche de cryptage aux cookies du navigateur que WordPress les utilisateurs stockent sur leurs machines locales. En gros, l'ajout de valeurs longues aléatoires à cet endroit rend votre site plus sécurisé. Visitez https:// api.wordpress. org/secret-key/1.1/salt/pour générer de manière aléatoire un ensemble de valeurs clés que vous pouvez copier et coller dans votre `wp-config.php` fichier. Pour coller du texte dans un terminal PuTTY, placez le curseur où vous voulez coller le texte et faites un clic droit avec votre souris dans le terminal PuTTY.

Pour plus d'informations sur les clés de sécurité, rendez-vous sur https://wordpress. org/ support/article/editing-wp-config-php/#security -clés.

> **Note**
>
> Les valeurs ci-dessous sont proposées à titre d'exemple seulement. N'utilisez pas ces valeurs pour votre installation.

```
define('AUTH_KEY',         ' #U$$+[RXN8:b^-L 0(WU_+ c+WFkI~c]o]-bHw+)/
Aj[wTwSiZ<Qb[mghEXcRh-');
define('SECURE_AUTH_KEY',  'Zsz._P=l/|y.Lq)XjlkwS1y5NJ76E6EJ.AV0pCKZZB,*~*r ?
6OP$eJT@;+(ndLg');
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',        'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:?0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT',        'C$DpB4Hj[JK:?{ql`sRVa:{:7yShy(9A@5wg+`JJVb1fk%_-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.${+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q1O-bp28EKv');
```

```
define('LOGGED_IN_SALT',    ';j{00P*owZf)kVD+FVLn-~ >.|Y%Ug4#I^*LVd9QeZ^&XmK|
e(76miC+&W&+^0P/');
define('NONCE_SALT',        '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/,.6[=UK<J_y9?JWG');
```

e. Enregistrez le fichier et quittez votre éditeur de texte.

Pour installer vos WordPress fichiers sous la racine du document Apache

- Maintenant que vous avez décompressé le dossier d'installation, créé une base de données et un utilisateur MySQL et personnalisé le fichier de WordPress configuration, vous êtes prêt à copier vos fichiers d'installation sur le document root de votre serveur Web afin de pouvoir exécuter le script d'installation qui complète votre installation. L'emplacement de ces fichiers varie selon que vous souhaitez que votre WordPress blog soit disponible à la racine de votre serveur Web (par exemple,*my.public.dns.amazonaws.com*) ou dans un sous-répertoire ou un dossier situé sous la racine (par exemple,*my.public.dns.amazonaws.com/blog*).
  - Si vous souhaitez exécuter WordPress à la racine de votre document, copiez le contenu du répertoire d'installation de WordPress (mais pas le répertoire lui-même) comme suit :

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

  - Si vous WordPress souhaitez exécuter dans un autre répertoire situé sous la racine du document, créez d'abord ce répertoire, puis copiez-y les fichiers. Dans cet exemple, s' WordPressexécutera à partir du répertoire `blog` :

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

> **Important**
>
> A des fins de sécurité, si vous ne passez pas à la prochaine procédure immédiatement, arrêtez le serveur web Apache (`httpd`) dès maintenant. Une fois que vous avez déplacé votre installation sous la racine du document Apache, le script WordPress d'installation n'est plus protégé et un attaquant pourrait accéder à votre blog si le serveur Web Apache était en cours d'exécution. Pour arrêter le serveur Web Apache, saisissez la commande sudo systemctl stop httpd. Si vous ne passez pas à la prochaine procédure, vous n'avez pas à arrêter le serveur web Apache.

Pour autoriser l'utilisation WordPress de permaliens

WordPress les permaliens doivent utiliser des `.htaccess` fichiers Apache pour fonctionner correctement, mais cela n'est pas activé par défaut sur Amazon Linux. Utilisez cette procédure pour permettre tous les remplacements à la racine du document Apache.

1. Ouvrez le fichier `httpd.conf` avec votre éditeur de texte préféré (comme nano ou vim). Si vous n'avez pas d'éditeur de texte préféré, `nano` convient aux débutants.

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

2. Trouvez la section qui commence par `<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. Modifiez la ligne `AllowOverride None` dans la section ci-dessus par `AllowOverride All`.

> **Note**
>
> Il existe plusieurs lignes `AllowOverride` dans ce fichier. Assurez-vous de modifier la ligne dans la section `<Directory "/var/www/html">`.

```
AllowOverride All
```

4. Enregistrez le fichier et quittez votre éditeur de texte.

Pour installer la bibliothèque de dessins graphiques PHP sur AL2

La bibliothèque GD pour PHP vous permet de modifier des images. Installez cette bibliothèque si vous devez recadrer l'image d'en-tête pour votre blog. La version phpMyAdmin que vous installez peut nécessiter une version minimale spécifique de cette bibliothèque (par exemple, la version 7.2).

Utilisez la commande suivante pour installer la bibliothèque de dessins graphiques PHP sur AL2. Par exemple, si vous avez installé php7.2 dans le amazon-linux-extras cadre de l'installation de la pile LAMP, cette commande installe la version 7.2 de la bibliothèque de dessins graphiques PHP.

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

Pour vérifier la version installée, utilisez la commande suivante :

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

Voici un exemple de sortie :

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

Pour corriger les autorisations sur les fichiers pour le serveur web Apache

Certaines des fonctionnalités disponibles WordPress nécessitent un accès en écriture à la racine du document Apache (comme le téléchargement de médias via les écrans d'administration). Si ce n'est pas déjà fait, appliquez les appartenances aux groupes et les autorisations suivantes (comme décrit plus en détail dans leTutoriel : Installation d'un serveur LAMP sur AL2).

1. Accordez la propriété du fichier `/var/www` et de son contenu à l'utilisateur `apache`.

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

2. Accordez la propriété de groupe de `/var/www` et de son contenu au groupe `apache`.

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

3. Modifiez les autorisations sur les répertoires de `/var/www` et ses sous-répertoires pour ajouter des autorisations d'écriture de groupe et définir l'ID de groupe pour les futurs sous-répertoires.

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

4. Modifiez de façon récursive les autorisations sur les fichiers de `/var/www` et ses sous-répertoires.

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
```

> **Note**
>
> Si vous avez l'intention de l'utiliser également WordPress en tant que serveur FTP, vous aurez besoin de paramètres de groupe plus permissifs ici. Pour ce faire, veuillez consulter les étapes recommandées et WordPress les paramètres de sécurité.

5. Redémarrez le serveur web Apache pour récupérer les nouveaux groupe et autorisations.

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

Exécutez le script WordPress d'installation avec AL2

Vous êtes prêt à procéder à l'installation WordPress. Les commandes que vous utilisez dépendent du système d'exploitation. Les commandes de cette procédure sont destinées à être utilisées avec AL2.

1. Utilisez la commande systemctl pour vous assurer que les services `httpd` et de base de données commencent à chaque démarrage système.

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

2. Vérifiez que le serveur de base de données est en cours d'exécution.

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

Si le service de base de données n'est pas en cours d'exécution, démarrez-le.

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

3. Vérifiez que votre serveur web Apache (`httpd`) est en cours d'exécution.

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

Si le service `httpd` n'est pas en cours d'exécution, démarrez-le.

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

4. Dans un navigateur Web, saisissez l'URL de votre WordPress blog (soit l'adresse DNS publique de votre instance, soit cette adresse suivie du `blog` dossier). Vous devriez voir le script WordPress d'installation. Fournissez les informations requises par l' WordPress installation. Choisissez Installer WordPress pour terminer l'installation. Pour plus d'informations, voir Étape 5 : Exécuter le script d'installation sur le WordPress site Web.

Étapes suivantes

Après avoir testé votre WordPress blog, pensez à mettre à jour sa configuration.

Utiliser un nom de domaine personnalisé

Si un nom de domaine est associé à l'adresse EIP de votre EC2 instance, vous pouvez configurer votre blog pour qu'il utilise ce nom au lieu de l'adresse DNS EC2 publique. Pour plus d'informations, voir Modification de l'URL du site sur le WordPress site Web.

Configurer votre blog

Vous pouvez configurer votre blog pour utiliser différents thèmes et plugins afin de proposer une expérience plus personnalisée à vos lecteurs. Cependant, il peut arriver que le processus d'installation échoue ce qui entraînera la perte de tout votre blog. Nous vous recommandons vivement de créer une sauvegarde de l'Amazon Machine Image (AMI) de votre instance avant d'essayer d'installer des thèmes ou des plugins. Ainsi, vous pouvez restaurer votre blog en cas

de problème pendant l'installation. Pour plus d'informations, consultez la section Création de votre propre AMI.

Augmenter la capacité

Si votre WordPress blog devient populaire et que vous avez besoin de plus de puissance de calcul ou de stockage, considérez les étapes suivantes :

- Développez l'espace de stockage sur votre instance. Pour plus d'informations, consultez la section Volumes Amazon EBS dans le Guide de l'utilisateur Amazon EC2.
- Déplacez votre base de données MySQL vers Amazon RDS pour profiter de la capacité du service à se mettre à l'échelle facilement.

Améliorer les performances réseau de votre trafic Internet

Si vous vous attendez à ce que votre blog génère du trafic provenant d'utilisateurs situés dans le monde entier, envisagez d'utiliser AWS Global Accelerator. Global Accelerator vous aide à réduire le temps de latence en améliorant les performances du trafic Internet entre les appareils clients de vos utilisateurs et votre WordPress application en cours d'exécution AWS. Global Accelerator utilise le réseau AWS mondial pour diriger le trafic vers un point de terminaison d'application sain dans la AWS région la plus proche du client.

En savoir plus sur WordPress

Pour plus d'informations WordPress, consultez la documentation d'aide du WordPress Codex à l'adresse http://codex.wordpress.org/.

Pour plus d'informations sur le dépannage de votre installation, consultez la section Problèmes d'installation courants.

Pour plus d'informations sur le renforcement de la sécurité de votre WordPress blog, consultez la section Renforcement WordPress.

Pour plus d'informations sur la gestion de votre WordPress blog up-to-date, consultez la section Mise à jour WordPress.

Aide! Mon nom DNS public a changé et mon blog ne fonctionne plus

Votre WordPress installation est automatiquement configurée à l'aide de l'adresse DNS publique de votre EC2 instance. Si vous arrêtez et redémarrez l'instance, l'adresse DNS publique change (sauf si

elle est associée à une adresse IP élastique) et votre blog ne fonctionnera plus car il fait référence à des ressources à une adresse qui n'existe plus (ou qui est attribuée à une autre EC2 instance). Une description plus détaillée du problème et plusieurs solutions possibles sont décrites dans la section Modification de l'URL du site.

Si cela est arrivé à votre WordPress installation, vous pourrez peut-être récupérer votre blog en suivant la procédure ci-dessous, qui utilise l'interface de ligne de wp-cli commande pour WordPress.

Pour modifier l'URL de votre WordPress site à l'aide du wp-cli

1. Connectez-vous à votre EC2 instance via SSH.
2. Notez l'ancienne URL de site et la nouvelle URL de site pour votre instance. L'ancienne URL du site est probablement le nom DNS public de votre EC2 instance lors de l'installation WordPress. La nouvelle URL du site est le nom DNS public actuel de votre EC2 instance. Si vous n'êtes pas certain de votre ancienne URL de site, vous pouvez utiliser curl pour la trouver avec la commande suivante.

   ```
   [ec2-user ~]$ curl localhost | grep wp-content
   ```

   Vous devriez voir des références à votre ancien nom DNS public dans les données de sortie qui ressembleront à cela (ancienne URL de site en rouge) :

   ```
   <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. Téléchargez le kit wp-cli avec la commande suivante.

   ```
   [ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/
   phar/wp-cli.phar
   ```

4. Recherchez et remplacez l'ancienne URL du site dans votre WordPress installation à l'aide de la commande suivante. Remplacez votre EC2 instance par l'ancien et le nouveau site URLs et par le chemin d'accès à votre WordPress installation (généralement `/var/www/html` ou `/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. Dans un navigateur Web, entrez l'URL du nouveau site de votre WordPress blog pour vérifier que le site fonctionne à nouveau correctement. Si ce n'est pas le cas, consultez les sections Modification de l'URL du site et Problèmes d'installation courants pour plus d'informations.

Utilisation d'Amazon Linux 2 en dehors d'Amazon EC2

Les images de AL2 conteneur peuvent être exécutées dans des environnements d'exécution de conteneurs compatibles.

AL2 peut également être exécuté en tant qu'invité virtualisé en dehors de l'exécution directe sur Amazon EC2.

> **Note**
>
> La configuration des AL2 images est différente de celle de AL2 023.
> Lors de la migration vers la AL2 version 023, assurez-vous de consulter la section Utiliser Amazon Linux 2023 en dehors d'Amazon EC2 et d'adapter votre configuration pour qu'elle soit compatible avec AL2 la version 023.

Exécuter AL2 en tant que machine virtuelle sur site

Utilisez les images de machine AL2 virtuelle (VM) pour le développement et les tests sur site. Nous proposons une image de AL2 machine virtuelle différente pour chacune des plateformes de virtualisation prises en charge. Vous pouvez consulter la liste des plateformes prises en charge sur la page des Images de machine virtuelle Amazon Linux 2.

Pour utiliser les images de machine AL2 virtuelle avec l'une des plateformes de virtualisation prises en charge, procédez comme suit :

- Étape 1 : Préparer l'image de démarrage seed.iso
- Étape 2 : Télécharger l'image de la machine virtuelle AL2
- Étape 3 : Démarrer et se connecter à votre nouvelle machine virtuelle

Étape 1 : Préparer l'image de démarrage `seed.iso`

L'image de démarrage `seed.iso` inclut les informations de configuration initiale requises pour démarrer votre nouvelle machine virtuelle, telles que la configuration réseau, le nom d'hôte et les données utilisateur.

> **Note**
>
> L'image de démarrage `seed.iso` inclut uniquement les informations de configuration requises pour démarrer la machine virtuelle. Il n'inclut pas les fichiers du système AL2 d'exploitation.

Pour générer l'image de démarrage `seed.iso`, vous avez besoin de deux fichiers de configuration :

- `meta-data` – Ce fichier inclut le nom d'hôte et les paramètres de réseau statique pour la machine virtuelle.
- `user-data` – Ce fichier configure les comptes utilisateur et spécifie leurs mots de passe, paires de clés et mécanismes d'accès. Par défaut, l'image de la AL2 machine virtuelle crée un compte `ec2-user` utilisateur. Vous utilisez le fichier de configuration `user-data` pour définir le mot de passe pour le compte utilisateur par défaut.

Pour créer le disque de démarrage **`seed.iso`**

1. Créez un dossier appelé `seedconfig` et accédez à celui-ci.
2. Créez le fichier de configuration `meta-data`.
   a. Créez un fichier nommé `meta-data`.
   b. Ouvrez le fichier `meta-data` à l'aide de l'éditeur de votre choix et ajoutez ce qui suit.

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

*`vm_hostname`*Remplacez-le par un nom d'hôte de machine virtuelle de votre choix et configurez les paramètres réseau selon les besoins.

c. Enregistrez et fermez le fichier de configuration `meta-data`.

Pour obtenir un exemple de fichier de configuration `meta-data` qui spécifie le nom d'hôte d'une machine virtuelle (`amazonlinux.onprem`), configure l'interface réseau par défaut (`eth0`) et spécifie les adresses IP statiques pour les périphériques réseau nécessaires, consultez l'exemple de fichier Seed.iso.

3. Créez le fichier de configuration `user-data`.

a. Créez un fichier nommé `user-data`.

b. Ouvrez le fichier `user-data` à l'aide de l'éditeur de votre choix et ajoutez ce qui suit.

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

*`plain_text_password`*Remplacez-le par le mot de passe de votre choix pour le compte `ec2-user` utilisateur par défaut.

c. (Facultatif) Par défaut, cloud-init applique les paramètres réseau à chaque démarrage de la machine virtuelle. Ajoutez ce qui suit pour empêcher cloud-init d'appliquer les paramètres réseau à chaque démarrage et conserver les paramètres réseau appliqués lors du premier démarrage.

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

d. Enregistrez et fermez le fichier de configuration `user-data`.

De même, vous pouvez créer des comptes d'utilisateur supplémentaires et spécifier leurs mécanismes d'accès, mots de passe et paires de clés. Pour plus d'informations sur les directives prises en charge, consultez la Référence du module. Pour obtenir un exemple de fichier `user-data` permettant de créer trois utilisateurs supplémentaires et de spécifier un mot de passe personnalisé pour le compte d'utilisateur `ec2-user` par défaut, consultez le fichier d'exemple Seed.iso.

4. Créez l'image de démarrage `seed.iso` en utilisant les fichiers de configuration `meta-data` et `user-data`.

   Pour Linux, utilisez un outil tel que genisoimage. Accédez au dossier `seedconfig` et exécutez la commande suivante.

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

   Pour macOS, utilisez un outil tel que hdiutil. Remontez d'un niveau à partir du dossier `seedconfig` et exécutez la commande suivante.

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

Étape 2 : Télécharger l'image de la machine virtuelle AL2

Nous proposons une image de AL2 machine virtuelle différente pour chacune des plateformes de virtualisation prises en charge. Vous pouvez consulter la liste des plateformes prises en charge et télécharger l'image de la machine virtuelle adéquate pour la plateforme choisie sur la page des Images de machine virtuelle Amazon Linux 2.

Étape 3 : Démarrer et se connecter à votre nouvelle machine virtuelle

Pour démarrer et vous connecter à votre nouvelle machine virtuelle, vous devez disposer de l'image de `seed.iso` démarrage (créée à l'étape 1) et d'une image de AL2 machine virtuelle (téléchargée à l'étape 2). Cette procédure varie selon la plateforme de machine virtuelle que vous choisissez.

VMware vSphere

L'image de machine virtuelle pour VMware est mise à disposition au format OVF.

Pour démarrer la machine virtuelle à l'aide de VMware vSphere

1. Créez une banque de données pour le fichier `seed.iso` ou ajoutez-la à une banque de données existante.
2. Déployez le modèle OVF, mais ne démarrez pas encore la machine virtuelle.
3. Dans le panneau Navigateur, cliquez avec le bouton droit sur la nouvelle machine virtuelle et choisissez Modifier les paramètres.
4. Sous l'onglet Matériel virtuel pour Nouvel appareil, choisissez Lecteur de CD/DVD, puis Ajouter.
5. Pour New CD/DVD Drive, choisissez le fichier ISO de la banque de données. Sélectionnez la banque de données à laquelle vous avez ajouté le fichier `seed.iso`, accédez au fichier `seed.iso` et sélectionnez-le, puis choisissez OK.
6. Pour New CD/DVD Drive, sélectionnez Connect, puis OK.

Après avoir associé la banque de données à la machine virtuelle, vous devriez pouvoir le démarrer.

KVM

Pour démarrer la machine virtuelle à l'aide de KVM

1. Ouvrez l'assistant Créer une machine virtuelle.
2. Pour l'étape 1, choisissez Importer une image disque existante.
3. Pour l'étape 2, accédez à l'image de la machine virtuelle et sélectionnez-la. Pour OS type (Type de système d'exploitation) et Version, choisissez respectivement Linux et Red Hat Enterprise Linux 7.0.
4. Pour l'étape 3, spécifiez la quantité de RAM et le nombre de RAM CPUs à utiliser.
5. Pour l'étape 4, entrez un nom pour la nouvelle machine virtuelle et sélectionnez Personnaliser la configuration avant l'installation, puis choisissez Terminer.
6. Dans la fenêtre Configuration de la machine virtuelle, choisissez Ajouter du matériel.
7. Dans la fenêtre Ajouter un nouveau matériel virtuel, choisissez Stockage.
8. Dans la configuration de stockage, choisissez Sélectionner ou créer un stockage personnalisé. Pour Type d'appareil, choisissez Appareil CDROM. Choisissez Gérer, Parcourir en local, puis accédez au fichier `seed.iso` et sélectionnez-le. Choisissez Finish.
9. Choisissez Commencer l'installation.

Oracle VirtualBox

Pour démarrer la machine virtuelle à l'aide d'Oracle VirtualBox

1. Ouvrez Oracle VirtualBox et choisissez Nouveau.
2. Dans Name (Nom), saisissez un nom descriptif pour la machine virtuelle et dans Type et Version, sélectionnez respectivement Linux et Red Hat (64 bits). Choisissez Continue.
3. Pour Memory size (Taille de la mémoire), spécifiez la quantité de mémoire à allouer à la machine virtuelle, puis choisissez Continue (Continuer).
4. Pour Hard disk (Disque dur), choisissez Use an existing virtual hard disk file (Utiliser un fichier de disque dur virtuel existant), recherchez et ouvrez l'image de machine virtuelle, puis choisissez Create (Créer).
5. Avant de démarrer la machine virtuelle, vous devez charger le fichier `seed.iso` dans le lecteur optique virtuel de la machine virtuelle :
   a. Sélectionnez la nouvelle machine virtuelle, choisissez Paramètres, puis Stockage.
   b. Dans la liste Storage Devices (Appareils de stockage), sous Controller: IDE (Contrôleur : IDE), choisissez le lecteur optique Empty (Vide).
   c. Dans la section Attributs du lecteur optique, cliquez sur le bouton Parcourir, sélectionnez Choisir un fichier de disque optique virtuel, puis sélectionnez le fichier `seed.iso`. Cliquez sur OK pour appliquer les modifications et fermer les paramètres.

Après avoir ajouté le fichier `seed.iso` au lecteur optique virtuel, vous devriez pouvoir démarrer la machine virtuelle.

Microsoft Hyper-V

L'image VM pour Microsoft Hyper-V est compressée dans un fichier zip. Vous devez extraire le contenu du fichier .zip.

Pour démarrer la machine virtuelle à l'aide de Microsoft Hyper-V

1. Ouvrez New Virtual Machine Wizard (Nouvel assistant de machine virtuelle).
2. Lorsque vous êtes invité à sélectionner une génération, sélectionnez Génération 1.
3. Lorsque vous êtes invité à configurer la carte réseau, pour Connexion, choisissez Externe.

4. Lorsque vous êtes invité à connecter un disque dur virtuel, choisissez Utiliser un disque dur virtuel existant, choisissez Parcourir, puis accédez à et sélectionnez l'image de la machine virtuelle. Choisissez Terminer pour créer la machine virtuelle.
5. Cliquez avec le bouton droit sur la nouvelle machine virtuelle et choisissez Paramètres. Dans la fenêtre Paramètres, sous Contrôleur IDE 1, choisissez Lecteur de DVD.
6. Pour le lecteur de DVD, choisissez Fichier Image, puis recherchez et sélectionnez le fichier `seed.iso`.
7. Appliquez les modifications et démarrez la machine virtuelle.

Après le démarrage de la machine virtuelle, connectez-vous avec l'un des comptes d'utilisateur définis dans le fichier de configuration `user-data`. Après la première connexion, vous pouvez déconnecter l'image de démarrage `seed.iso` de la machine virtuelle.

Identification des instances et des versions d'Amazon Linux

Il peut être important de pouvoir déterminer quelle distribution Linux et quelle version de cette distribution est une image ou une instance de système d'exploitation. Amazon Linux fournit des mécanismes permettant d'identifier Amazon Linux par rapport aux autres distributions Linux, ainsi que de déterminer de quelle version d'Amazon Linux il s'agit de l'image.

Cette section couvre les différentes méthodes qui peuvent être utilisées, leurs limites, et passe en revue quelques exemples de leur utilisation.

Rubriques

Utilisation de la `os-release` norme

Amazon Linux est conforme à la `os-releasenorme` d'identification des distributions Linux. Ce fichier fournit des informations lisibles par machine concernant l'identification du système d'exploitation et les informations de version.

> **Note**
>
> La norme indique que `/etc/os-release` l'analyse doit être tentée en premier, suivie de. `/usr/lib/os-release` Il faut veiller à suivre la norme concernant les noms et les chemins des fichiers.

Rubriques

Principales différences d'identification

Le se `os-release` trouve à`/etc/os-release`, et s'il n'est pas présent, à`/usr/lib/os-release`. Consultez la os-releasenorme pour obtenir des informations complètes.

La méthode la plus fiable pour déterminer si une instance exécute Amazon Linux est de cocher le `ID` champ`os-release`.

Le moyen le plus fiable de faire la distinction entre les versions consiste à cocher le `VERSION_ID` champ dans `os-release` :

- AMI Amazon Linux : `VERSION_ID` contient une version basée sur la date (par exemple,`2018.03`)
- AL2: `VERSION_ID="2"`
- AL2023 : `VERSION_ID="2023"`

> **Note**
>
> N'oubliez pas qu'`VERSION_ID`il s'agit d'un champ lisible par machine destiné à un usage programmatique, alors qu'`PRETTY_NAME`il est conçu pour être affiché aux utilisateurs. Consultez the section called “Types de champs” pour plus d'informations sur les types de champs.

Types de champs : lisibles par machine ou lisibles par l'homme

Le `/etc/os-release` fichier (ou `/usr/lib/os-release` s'il `/etc/os-release` n'existe pas) contient deux types de champs : les champs lisibles par machine destinés à un usage programmatique et les champs lisibles par l'homme destinés à être présentés aux utilisateurs.

Champs lisibles par machine

Ces champs utilisent des formats standardisés et sont destinés à être traités par des scripts, des gestionnaires de packages et d'autres outils automatisés. Ils ne contiennent que des lettres minuscules, des chiffres et une ponctuation limitée (points, traits de soulignement et tirets).

- `ID`— Identifiant du système d'exploitation. Amazon Linux `amzn` l'utilise dans toutes les versions, ce qui le distingue des autres distributions telles que Debian (`debian`), Ubuntu (`ubuntu`) ou Fedora () `fedora`

- `VERSION_ID`— Version du système d'exploitation pour une utilisation programmatique (par exemple,`2023`)
- `ID_LIKE`— Liste séparée par des espaces des distributions associées (par exemple,) `fedora`
- `VERSION_CODENAME`— Nom de code de publication pour les scripts (par exemple,) `karoo`
- `VARIANT_ID`— Identifiant de variante pour les décisions programmatiques
- `BUILD_ID`— Identifiant de build pour les images du système
- `IMAGE_ID`— Identifiant d'image pour les environnements conteneurisés
- `PLATFORM_ID`— Identifiant de plateforme (par exemple,`platform:al2023`)

Champs lisibles par l'homme

Ces champs sont destinés à être affichés aux utilisateurs et peuvent contenir des espaces, des majuscules et du texte descriptif. Ils doivent être utilisés lors de la présentation des informations du système d'exploitation dans les interfaces utilisateur.

- `NAME`— Nom du système d'exploitation à afficher (par exemple,`Amazon Linux`)
- `PRETTY_NAME`— Nom complet du système d'exploitation avec version à afficher (par exemple,`Amazon Linux 2023.8.20250721`)
- `VERSION`— Informations de version adaptées à la présentation par l'utilisateur
- `VARIANT`— Nom de la variante ou de l'édition à afficher (par exemple,`Server Edition`)

Autres champs d'information

Ces champs fournissent des métadonnées supplémentaires sur le système d'exploitation :

- `HOME_URL`— URL de la page d'accueil du projet
- `DOCUMENTATION_URL`— URL de la documentation
- `SUPPORT_URL`— URL des informations de support
- `BUG_REPORT_URL`— URL de signalement de bogue
- `VENDOR_NAME`— Nom du fournisseur
- `VENDOR_URL`— URL du fournisseur
- `SUPPORT_END`— End-of-support date au YYYY-MM-DD format
- `CPE_NAME`— Identifiant d'énumération de plate-forme commune

- `ANSI_COLOR`— Code couleur ANSI pour l'affichage du terminal

Lorsque vous écrivez des scripts ou des applications qui doivent identifier Amazon Linux par programmation, utilisez les champs lisibles par machine tels que et. `ID` `VERSION_ID` Lorsque vous affichez des informations sur le système d'exploitation aux utilisateurs, utilisez des champs lisibles par l'homme tels que`PRETTY_NAME`.

Exemples pour l'**`/etc/os-release`**

Le contenu du `/etc/os-release` fichier varie selon les versions d'Amazon Linux :

AL2023

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

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

AL2

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

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

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

Amazon Linux AMI

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

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

Comparaison avec d'autres distributions

Pour comprendre comment Amazon Linux s'intègre dans l'écosystème Linux au sens large, comparez son `/etc/os-release` format à celui d'autres distributions majeures :

Fedora

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

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

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

Debian

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

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

Ubuntu

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

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

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

Remarquez comment les champs lisibles par machine fournissent une identification cohérente entre les distributions :

- `ID`— Identifie de manière unique le système d'exploitation : `amzn` pour Amazon Linux, `fedora` pour Fedora, `debian` pour Debian, `ubuntu` pour Ubuntu
- `ID_LIKE`— Affiche les relations de distribution : Amazon Linux utilise `fedora` (AL2023) ou `centos rhel fedora` (AL2), tandis qu'Ubuntu affiche `debian` pour indiquer son héritage Debian
- `VERSION_ID`— Fournit des informations de version analysables par machine : `2023` pour AL2 023, pour Fedora, `42` pour Debian, pour Ubuntu `12` `24.04`

En revanche, les champs lisibles par l'homme sont conçus pour être affichés aux utilisateurs :

- `NAME`— Nom du système d'exploitation convivial :`Amazon Linux`,`Fedora Linux`,`Debian GNU/Linux`, `Ubuntu`
- `PRETTY_NAME`— Nom d'affichage complet avec version :`Amazon Linux 2023.8.20250721`,`Fedora Linux 42 (Container Image)`,`Debian GNU/Linux 12 (bookworm)`, `Ubuntu 24.04.2 LTS`
- `VERSION`— Version lisible par l'homme avec un contexte supplémentaire tel que des noms de code ou des types de versions

Lorsque vous écrivez des scripts multiplateformes, utilisez toujours les champs lisibles par machine (`ID`,`VERSION_ID`,`ID_LIKE`) pour la logique et les décisions, et utilisez les champs lisibles par l'homme (`PRETTY_NAME`,`NAME`) uniquement pour afficher des informations aux utilisateurs.

Spécifique à Amazon Linux

Certains fichiers spécifiques à Amazon Linux peuvent être utilisés pour identifier Amazon Linux et sa version. Le nouveau code doit utiliser la `/etc/os-release` norme afin d'être compatible avec les distributions croisées. L'utilisation de fichiers spécifiques à Amazon Linux est déconseillée.

Rubriques

le fichier `/etc/system-release` ;

Amazon Linux contient un fichier `/etc/system-release` qui spécifie la version actuelle qui est installée. Ce fichier est mis à jour à l'aide des gestionnaires de packages et sur Amazon, Linux fait partie du `system-release` package. Bien que certaines autres distributions comme Fedora aient également ce fichier, il n'est pas présent dans les distributions basées sur Debian comme Ubuntu.

> **Note**
>
> Le `/etc/system-release` fichier contient une chaîne lisible par l'homme et ne doit pas être utilisé par programmation pour identifier un système d'exploitation ou une version. Utilisez plutôt les champs lisibles par machine `/etc/os-release` (ou `/usr/lib/os-release` s'ils `/etc/os-release` n'existent pas).

Amazon Linux contient également une version lisible par machine `/etc/system-release` qui suit la spécification CPE (Common Platform Enumeration) figurant dans le fichier. `/etc/system-release-cpe`

Fichier d'identification d'image

Chaque image Amazon Linux contient un `/etc/image-id` fichier unique qui fournit des informations supplémentaires sur l'image d'origine telle que générée par l'équipe Amazon Linux. Ce fichier est spécifique à Amazon Linux et ne se trouve pas dans d'autres distributions Linux telles que Debian, Ubuntu ou Fedora. Ce fichier contient les informations suivantes sur l'image :

- `image_name`,`image_version`, `image_arch` — Valeurs issues de la recette de construction utilisée pour créer l'image.
- `image_stamp` — Valeur hexadécimale aléatoire unique qui a été générée pendant la création de l'image.
- `image_date`— L'heure UTC de création de l'image, au YYYYMMDDhhmmssformat.
- `recipe_name`, `recipe_id` — Le nom et l'ID de la recette de construction utilisée pour créer l'image.

Exemples de fichiers spécifiques à Amazon Linux

Les sections suivantes fournissent des exemples de fichiers d'identification spécifiques à Amazon Linux pour chaque version majeure d'Amazon Linux.

> **Note**
>
> Dans n'importe quel code du monde réel, `/usr/lib/os-release` doit être utilisé si le `/etc/os-release` fichier n'existe pas.

AL2023

Les exemples suivants montrent les fichiers d'identification pour AL2 023.

Exemple de `/etc/image-id` pour AL2 023 :

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

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

Exemple de `/etc/system-release` pour AL2 023 :

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

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

AL2

Les exemples suivants présentent les fichiers d'identification pour AL2.

Exemple de `/etc/image-id` pour AL2 :

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

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

Exemple de `/etc/system-release` pour AL2 :

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

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

AMI Amazon Linux

Les exemples suivants présentent les fichiers d'identification de l'AMI Amazon Linux.

Exemple d'AMI `/etc/image-id` pour Amazon Linux :

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

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

Exemple d'AMI `/etc/system-release` pour Amazon Linux :

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

```
Amazon Linux AMI release 2018.03
```

Exemple de code pour la détection du système d'exploitation

Les exemples suivants montrent comment détecter par programmation le système d'exploitation et sa version à l'aide du fichier `/etc/os-release` (ou `/usr/lib/os-release` s'il `/etc/os-release` n'existe pas). Ces exemples montrent comment faire la distinction entre Amazon Linux et les autres distributions, ainsi que comment utiliser le `ID_LIKE` champ pour déterminer les familles de distribution.

Le script ci-dessous est implémenté dans plusieurs langages de programmation différents, et chaque implémentation produira le même résultat.

Shell

```
#!/bin/bash

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

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

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

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

```
}

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

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

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

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

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

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

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

```
echo "Detailed OS Information:"
echo "======================="
echo "ID: $ID"
echo "VERSION_ID: $VERSION_ID"
echo "PRETTY_NAME: $PRETTY_NAME"
[ -n "$ID_LIKE" ] && echo "ID_LIKE: $ID_LIKE"

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

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

Python 3.7-3.9

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

import os
import sys

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

    # Try /etc/os-release first, then /usr/lib/os-release
```

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

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

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

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

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

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

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

def is_like_debian(os_data):
    """Check if this is like Debian (includes Ubuntu and derivatives)."""
    if os_data.get('ID') == 'debian':
```

```
        return True
    id_like = os_data.get('ID_LIKE', '')
    return 'debian' in id_like

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

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

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

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

        # Check for Amazon Linux specific files
```

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

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

Python 3.10+

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

import os
import sys
import platform

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

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

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

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

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

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

```
def main():
    # Parse os-release file using the standard library function (Python 3.10+)
    try:
        os_data = platform.freedesktop_os_release()
    except OSError:
        print("Error: os-release file not found")
        sys.exit(1)

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

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

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

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

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

Perl

```
#!/usr/bin/env perl

use strict;
use warnings;

# Function to parse the os-release file and return a hash of key-value pairs
sub parse_os_release {
    my %os_release_data;

    # Try /etc/os-release first, then /usr/lib/os-release
    my @paths = ('/etc/os-release', '/usr/lib/os-release');

    for my $path (@paths) {
        if (-f $path) {
            if (open(my $fh, '<', $path)) {
                while (my $line = <$fh>) {
                    chomp $line;
                    next if $line =~ /^\s*$/ || $line =~ /^\s*#/;

                    if ($line =~ /^([^=]+)=(.*)$/) {
                        my ($key, $value) = ($1, $2);
                        # Remove quotes if present
                        $value =~ s/^["']|["']$//g;
                        $os_release_data{$key} = $value;
                    }
                }
                close($fh);
                return %os_release_data;
            }
        }
    }

    die "Error: os-release file not found\n";
}
```

```
# Function to check if this is Amazon Linux
sub is_amazon_linux {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'amzn';
}

# Function to check if this is Fedora
sub is_fedora {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'fedora';
}

# Function to check if this is Ubuntu
sub is_ubuntu {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'ubuntu';
}

# Function to check if this is Debian
sub is_debian {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'debian';
}

# Function to check if this is like Fedora (includes Amazon Linux, CentOS, RHEL,
 etc.)
sub is_like_fedora {
    my %os_data = @_;
    return 1 if ($os_data{ID} // '') eq 'fedora';
    my $id_like = $os_data{ID_LIKE} // '';
    return $id_like =~ /fedora/;
}

# Function to check if this is like Debian (includes Ubuntu and derivatives)
sub is_like_debian {
    my %os_data = @_;
    return 1 if ($os_data{ID} // '') eq 'debian';
    my $id_like = $os_data{ID_LIKE} // '';
    return $id_like =~ /debian/;
}

# Main execution
my %os_data = parse_os_release();
```

```
# Display results
print "Operating System Detection Results:\n";
print "==================================\n";
print "Is Amazon Linux: " . (is_amazon_linux(%os_data) ? "YES" : "NO") . "\n";
print "Is Fedora: " . (is_fedora(%os_data) ? "YES" : "NO") . "\n";
print "Is Ubuntu: " . (is_ubuntu(%os_data) ? "YES" : "NO") . "\n";
print "Is Debian: " . (is_debian(%os_data) ? "YES" : "NO") . "\n";
print "Is like Fedora: " . (is_like_fedora(%os_data) ? "YES" : "NO") . "\n";
print "Is like Debian: " . (is_like_debian(%os_data) ? "YES" : "NO") . "\n";
print "\n";

# Additional information
print "Detailed OS Information:\n";
print "========================\n";
print "ID: " . ($os_data{ID} // '') . "\n";
print "VERSION_ID: " . ($os_data{VERSION_ID} // '') . "\n";
print "PRETTY_NAME: " . ($os_data{PRETTY_NAME} // '') . "\n";
print "ID_LIKE: " . ($os_data{ID_LIKE} // '') . "\n" if $os_data{ID_LIKE};

# Amazon Linux specific information
if (is_amazon_linux(%os_data)) {
    print "\n";
    print "Amazon Linux Version Details:\n";
    print "=============================\n";
    my $version_id = $os_data{VERSION_ID} // '';

    if ($version_id eq '2018.03') {
        print "Amazon Linux AMI (version 1)\n";
    } elsif ($version_id eq '2') {
        print "Amazon Linux 2\n";
    } elsif ($version_id eq '2023') {
        print "Amazon Linux 2023\n";
    } else {
        print "Unknown Amazon Linux version: $version_id\n";
    }

    # Check for Amazon Linux specific files
    if (-f '/etc/image-id') {
        print "Amazon Linux image-id file present\n";
    }
}
```

Lorsqu'il est exécuté sur différents systèmes, le script produit le résultat suivant :

AL2023

```
Operating System Detection Results:
===================================
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
========================
ID: amzn
VERSION_ID: 2023
PRETTY_NAME: Amazon Linux 2023.8.20250721
ID_LIKE: fedora

Amazon Linux Version Details:
=============================
Amazon Linux 2023
Amazon Linux image-id file present
```

AL2

```
Operating System Detection Results:
===================================
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
========================
ID: amzn
VERSION_ID: 2
PRETTY_NAME: Amazon Linux 2
ID_LIKE: centos rhel fedora
```

```
Amazon Linux Version Details:
============================
Amazon Linux 2
Amazon Linux image-id file present
```

Amazon Linux AMI

```
Operating System Detection Results:
==================================
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=======================
ID: amzn
VERSION_ID: 2018.03
PRETTY_NAME: Amazon Linux AMI 2018.03
ID_LIKE: rhel fedora

Amazon Linux Version Details:
============================
Amazon Linux AMI (version 1)
Amazon Linux image-id file present
```

Ubuntu

```
Operating System Detection Results:
==================================
Is Amazon Linux: NO
Is Fedora: NO
Is Ubuntu: YES
Is Debian: NO
Is like Fedora: NO
Is like Debian: YES

Detailed OS Information:
=======================
ID: ubuntu
VERSION_ID: 24.04
```

```
PRETTY_NAME: Ubuntu 24.04.2 LTS
ID_LIKE: debian
```

Debian

```
Operating System Detection Results:
===================================
Is Amazon Linux: NO
Is Fedora: NO
Is Ubuntu: NO
Is Debian: YES
Is like Fedora: NO
Is like Debian: YES

Detailed OS Information:
========================
ID: debian
VERSION_ID: 12
PRETTY_NAME: Debian GNU/Linux 12 (bookworm)
```

Fedora

```
Operating System Detection Results:
===================================
Is Amazon Linux: NO
Is Fedora: YES
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
========================
ID: fedora
VERSION_ID: 42
PRETTY_NAME: Fedora Linux 42 (Container Image)
```

AWSintégration dans AL2

AWSoutils de ligne de commande

The AWS Command Line Interface (AWS CLI) est un outil open source qui fournit une interface cohérente pour interagir à l'Services AWSaide de commandes dans votre interface de ligne de commande. Pour plus d'informations, voir Qu'est-ce que le AWS Command Line Interface ? dans le guide de AWS Command Line Interface l'utilisateur.

AL2 et AL1 ont la version 1 du AWS CLI préinstallée. La version actuelle d'Amazon Linux, AL2 023, contient la version 2 AWS CLI préinstallée. Pour plus d'informations sur l'utilisation du AWS CLI on AL2 023, consultez Get started with AL2 023 dans le guide de l'utilisateur Amazon Linux 2023.

Premiers pas avec les environnements d'exécution de programmation

AL2 fournit différentes versions de certains environnements d'exécution linguistiques. Nous travaillons avec des projets en amont, tels que PHP, qui prennent en charge plusieurs versions en même temps. Pour obtenir des informations sur l'installation et la gestion de ces packages dont le nom est versionné, utilisez la `yum` commande pour rechercher et installer ces packages. Pour de plus amples informations, veuillez consulter Référentiel de packages.

Les rubriques suivantes décrivent le fonctionnement de chaque langage d'exécution dans AL2.

Rubriques

- CC++, et Fortran dans AL2
- Entrez AL2
- Javadans AL2
- Perldans AL2
- PHPdans AL2
- Pythondans AL2
- Rust in AL2

CC++, et Fortran dans AL2

AL2 inclut à la fois la collection de compilateurs GNU (GCC) et le Clang frontend pour. LLVM

La version majeure de GCC restera constante pendant toute la durée de vie de AL2. Les correctifs de bogues et de sécurité peuvent être rétroportés vers la version majeure de GCC celle qui est livrée. AL2

Par défaut, AL2 inclut la version 7.3 GCC qui construit presque tous les packages. Le `gcc10` package met GCC 10 à disposition dans une mesure limitée, mais nous ne recommandons pas d'en utiliser GCC 10 pour créer des packages.

Les indicateurs du compilateur par défaut qui compilent AL2 RPMs incluent des indicateurs d'optimisation et de renforcement. Nous vous recommandons d'inclure des indicateurs d'optimisation et de renforcement si vous créez votre propre code avecGCC.

Le compilateur par défaut et les indicateurs d'optimisation dans AL2 023 améliorent ce qui est présent dans AL2.

Entrez AL2

Vous souhaiterez peut-être créer votre propre code écrit Gosur Amazon Linux à l'aide d'une chaîne d'outils fournie avec AL2.

La Go chaîne d'outils sera mise à jour tout au long de la durée de vie de AL2. Cela peut être une réponse à un CVE de la chaîne d'outils que nous expédions, ou une condition préalable pour traiter un CVE dans un autre package.

Goest un langage de programmation qui évolue relativement rapidement. Il peut arriver que des applications existantes écrites Go doivent s'adapter aux nouvelles versions de la Go chaîne d'outils. Pour plus d'informations surGo, voir Go1 et l'avenir des Go programmes.

Bien qu'elle AL2 incorporera de nouvelles versions de la Go chaîne d'outils au cours de sa durée de vie, celle-ci ne sera pas synchronisée avec les versions en amontGo. Par conséquent, l'utilisation de la Go chaîne d'outils fournie AL2 peut ne pas être appropriée si vous souhaitez créer Go du code en utilisant les fonctionnalités de pointe du Go langage et de la bibliothèque standard.

Pendant la durée de vie de AL2, les versions antérieures des packages ne sont pas supprimées des référentiels. Si une Go chaîne d'outils antérieure est requise, vous pouvez choisir de ne pas corriger les bogues et de sécurité des nouvelles Go chaînes d'outils et d'installer une version antérieure à partir des référentiels en utilisant les mêmes mécanismes disponibles pour tous les RPM.

Si vous souhaitez créer votre propre Go code, AL2 vous pouvez utiliser la Go chaîne d'outils incluse en sachant que cette chaîne AL2 d'outils peut évoluer au cours de la durée de vie de. AL2

Javadans AL2

AL2 fournit plusieurs versions d'Amazon Corretto pour prendre en Java charge les charges de travail basées, ainsi que certaines versions. OpenJDK Nous vous recommandons de migrer vers Amazon Corretto en vue de la migration vers 023. AL2

Corretto est une version du kit de développement Open Java (OpenJDK) avec le support à long terme de. Amazon Corretto est certifié à l'aide du kit de compatibilité technique Java (TCK) pour garantir qu'il répond à Java la norme SE et qu'il est disponible surLinux, et. Windows macOS

Un package Amazon Corretto est disponible pour Corretto 1.8.0, Corretto 11 et Corretto 17.

Chaque version de Corretto est prise AL2 en charge pendant la même période que la version Corretto, ou jusqu'à la fin de vie de, selon la première éventualité. AL2 Pour plus d'informations, consultez le Amazon Corretto FAQs.

Perldans AL2

AL2 fournit la version 5.16 du langage de Perlprogrammation.

Perlmodules dans AL2

Les différents Perl modules sont conditionnés tels RPMs quels AL2. Bien qu'il existe de nombreux Perl modules disponibles RPMs, Amazon Linux n'essaie pas de regrouper tous les Perl modules possibles. Les modules sont conçus de manière RPMs à être utilisés par les packages RPM d'autres systèmes d'exploitation. Amazon Linux veillera donc en priorité à ce qu'ils soient dotés de correctifs de sécurité plutôt qu'à de pures mises à jour de fonctionnalités.

AL2 inclut également `CPAN` afin que Perl les développeurs puissent utiliser le gestionnaire de packages idiomatique pour les Perl modules.

PHPdans AL2

AL2 fournit actuellement deux versions entièrement prises en charge du langage de PHPprogrammation dans le cadre deAL2 Bibliothèque d'extras. Chaque PHP version est prise en charge pendant la même période qu'en amont, PHP comme indiqué sous la date d'obsolescence dans. Liste des extras d'Amazon Linux 2

Pour plus d'informations sur l'utilisation d' AL2 Extras pour installer des mises à jour d'applications et de logiciels sur vos instances, consultezAL2 Bibliothèque d'extras.

Pour faciliter la migration vers AL2 023, les versions PHP 8.1 et 8.2 sont disponibles sur AL2 et AL2 023.

> **Note**
>
> AL2 inclut PHP 7,1, 7,2, 7,3 et 7,4 `amazon-linux-extras` pouces Tous ces extras sont en fin de vie et il n'est pas garanti qu'ils obtiennent des mises à jour de sécurité supplémentaires. Pour savoir à quel moment chaque version de PHP est obsolète dans AL2, consultez le. Liste des extras d'Amazon Linux 2

Migration depuis des versions PHP 8.x antérieures

La PHP communauté en amont a élaboré une documentation de migration complète pour passer de PHP 8.1 à PHP 8.2. Il existe également de la documentation pour la migration de la PHP version 8.0 vers la version 8.1.

AL2 inclut les PHP versions 8.0, 8.1 et 8.2 `amazon-linux-extras` qui permettent une mise à niveau efficace vers la version AL2 023. Pour savoir à quel moment chaque version de PHP est obsolète dans AL2, consultez le. Liste des extras d'Amazon Linux 2

Migration à partir des versions PHP 7.x

La PHP communauté en amont a élaboré une documentation de migration complète pour passer de la version PHP 7.4 à la PHP version 8.0. Combinée à la documentation référencée dans la section précédente sur la migration vers les PHP versions 8.1 et PHP 8.2, vous disposez de toutes les étapes nécessaires pour migrer votre application PHP basée vers une version modernePHP.

Le PHPprojet tient à jour une liste et un calendrier des versions prises en charge, ainsi qu'une liste des branches non prises en charge.

> **Note**
>
> Lorsque la version AL2 023 a été publiée, toutes les versions 7.x et 5.x n'PHPétaient pas prises en charge par la PHPcommunauté et n'étaient pas incluses en tant qu'options dans la version 023. AL2

Pythondans AL2

AL2 fournit des correctifs de support et de sécurité pour la Python version 2.7 jusqu'en juin 2026, dans le cadre de notre engagement de support à long terme pour les packages AL2 principaux. Ce soutien va au-delà de la déclaration Python communautaire en amont de Python 2,7 EOL de janvier 2020.

> **Note**
>
> AL2023 complètement supprimé Python 2.7. Tous les composants Python requis sont désormais écrits pour fonctionner avec Python 3.

AL2 utilise le gestionnaire de `yum` paquets qui dépend fortement de la version Python 2.7. En version AL2 023, le gestionnaire de `dnf` packages a migré vers la version Python 3 et n'a plus besoin Python de la version 2.7. AL2023 est complètement passé à Python 3. Nous vous recommandons de terminer votre migration vers la version Python 3.

Rust in AL2

Vous voudrez peut-être créer votre propre code écrit à AL2 l'aide Rustd'une chaîne d'outils fournie avec AL2.

La Rust chaîne d'outils sera mise à jour tout au long de la durée de vie de AL2. Cela peut être en réponse à un CVE dans la chaîne d'outils que nous expédions, ou comme condition préalable à une mise à jour CVE dans un autre package.

Rustest un langage qui évolue relativement rapidement, avec des nouvelles sorties au rythme d'environ six semaines. Les nouvelles versions peuvent ajouter un nouveau langage ou des fonctionnalités de bibliothèque standard. Bien qu'elle AL2 incorporera de nouvelles versions de la Rust chaîne d'outils au cours de sa durée de vie, celle-ci ne sera pas synchronisée avec les versions en amontRust. Par conséquent, l'utilisation de la Rust chaîne d'outils fournie dans AL2 ce document peut ne pas être appropriée si vous souhaitez créer Rust du code en utilisant les fonctionnalités de pointe du Rust langage.

Pendant la durée de vie de AL2, les versions précédentes des packages ne sont pas supprimées des référentiels. Si une ancienne Rust chaîne d'outils est requise, vous pouvez choisir de ne pas corriger les bogues et de sécurité des nouvelles Rust chaînes d'outils et d'installer une version précédente à partir des référentiels en utilisant les mêmes processus disponibles pour tous les RPM.

Pour créer votre propre Rust code AL2, utilisez la chaîne d'Rustoutils incluse en sachant que cette chaîne AL2 d'outils peut évoluer tout au long de la durée de vie de. AL2

AL2 noyau

AL2 initialement livré avec un noyau 4.14, avec la version 5.10 comme version par défaut actuelle. Si vous utilisez toujours un noyau 4.14, nous vous conseillons de migrer vers le noyau 5.10.

La mise à jour dynamique du noyau est prise en charge sur AL2.

Rubriques

AL2 noyaux pris en charge

Versions du noyau prises en charge

Actuellement, AL2 AMIs ils sont disponibles avec les versions 4.14 et 5.10 du noyau, avec la version 5.10 par défaut. Nous vous recommandons d'utiliser une AL2 AMI avec le noyau 5.10.

AL2023 AMIs sont disponibles avec la version 6.1 du noyau. Pour plus d'informations, consultez la section AL2023 Modifications apportées au noyau AL2 dans le guide de l'utilisateur Amazon Linux 2023.

Période de prise en charge

Le noyau 5.10 disponible sur AL2 sera pris en charge jusqu'à ce que l' AL2 AMI atteigne la fin du support standard.

Prise en charge des correctifs en direct

AL2 version du noyau	Les correctifs en direct du noyau sont pris en charge
4,14	Oui
5,10	Oui
5,15	Non

Kernel Live Patching est activé AL2

> **Important**
>
> Amazon Linux mettra fin à la mise à jour en direct pour AL2 Kernel 4.14 le 31 octobre 2025. Les clients sont invités à utiliser le noyau 5.10 comme noyau par défaut pour AL2 (voir les noyaux AL2 pris en charge) ou à passer au AL2 023 avec les noyaux 6.1 et 6.12.
> Amazon Linux fournira des correctifs actifs pour le AL2 noyau 5.10 jusqu'à la fin de vie du 30 AL2 juin 2020.

Kernel Live Patching for vous AL2 permet d'appliquer une vulnérabilité de sécurité spécifique et des correctifs de bogues critiques à un noyau Linux en cours d'exécution, sans redémarrage ni interruption de l'exécution des applications. Cela vous permet de bénéficier d'une meilleure disponibilité des services et des applications, tout en appliquant ces correctifs jusqu'à ce que le système puisse être redémarré.

Pour plus d'informations sur Kernel Live Patching pour AL2 023, consultez Kernel Live Patching on AL2 023 dans le Guide de l'utilisateur Amazon Linux 2023.

AWS publie deux types de patchs dynamiques du noyau pour AL2 :

- Mises à jour de sécurité : incluent des mises à jour pour les failles et vulnérabilités communes (CVE) Linux. Ces mises à jour sont généralement jugées importantes ou critiques à l'aide des évaluations Amazon Linux de sécurité. Elles correspondent généralement à un score CVSS (Common Vulnerability Scoring System) égal à 7 ou plus. Dans certains cas, AWS peut fournir des mises à jour avant qu'un CVE ne soit attribué. Dans ces cas, les correctifs peuvent apparaître comme des correctifs de bogues.
- Corrections de bogues — Incluez des correctifs pour les bogues critiques et les problèmes de stabilité qui ne sont pas associés à CVEs.

AWS fournit des correctifs dynamiques du AL2 noyau pour une version du noyau jusqu'à 3 mois après sa publication. Après la période de 3 mois, vous devez effectuer une mise à jour vers une version ultérieure du noyau pour continuer à recevoir les correctifs à chaud du noyau.

AL2 les correctifs dynamiques du noyau sont disponibles sous forme de packages RPM signés dans les AL2 référentiels existants. Les correctifs peuvent être installés sur des instances individuelles à

l'aide des flux de travail yum existants, ou ils peuvent être installés sur un groupe d'instances gérées à l'aide de AWS Systems Manager.

L'activation de Kernel Live Patching AL2 est fournie sans frais supplémentaires.

Rubriques

Configurations et conditions préalables prises en charge

Kernel Live Patching est pris en charge sur les EC2 instances Amazon et les machines virtuelles sur site en cours d'exécution. AL2

Pour utiliser Kernel Live Patching sur Kernel AL2, vous devez utiliser :

- Version `4.14` ou `5.10` du noyau sur l'architecture `x86_64`
- Version `5.10` du noyau sur l'architecture `ARM64`

Exigences des politiques

Pour télécharger des packages depuis les référentiels Amazon Linux, Amazon EC2 doit avoir accès à des compartiments Amazon S3 appartenant au service. Si vous utilisez un point de terminaison Amazon Virtual Private Cloud (VPC) pour Amazon S3 dans votre environnement, vous devez vous assurer que votre politique de point de terminaison d'un VPC autorise l'accès à ces compartiments publics.

Le tableau décrit chacun des compartiments Amazon S3 auxquels il EC2 peut être nécessaire d'accéder pour Kernel Live Patching.

ARN de compartiment S3	Description
arn:aws:s3 : ::packages. *region*.amazonaws.com/*	Compartiment Amazon S3 contenant des packages d'AMI Amazon Linux

ARN de compartiment S3	Description
arn:aws:s3 : ::repo. *region*.amazonaws.com/*	Compartiment Amazon S3 contenant des référentiels d'AMI Amazon Linux
arn:aws:s3 : ::amazonlinux. *region*.amazonaws.com/*	Compartiment Amazon S3 contenant des AL2 référentiels
arn:aws:s3 : ::amazonlinux-2-repos- /* *region*	Compartiment Amazon S3 contenant des AL2 référentiels

La politique suivante illustre comment restreindre l'accès aux identités et aux ressources qui appartiennent à votre organisation et fournir l'accès aux compartiments Amazon S3 requis pour le Kernel Live Patching. Remplacez*region*, *principal-org-id* et *resource-org-id* par les valeurs de votre organisation.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRequestsByOrgsIdentitiesToOrgsResources",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "principal-org-id",
          "aws:ResourceOrgID": "resource-org-id"
        }
      }
    },
    {
      "Sid": "AllowAccessToAmazonLinuxAMIRepositories",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::packages.region.amazonaws.com/*",
        "arn:aws:s3:::repo.region.amazonaws.com/*",
        "arn:aws:s3:::amazonlinux.region.amazonaws.com/*",
        "arn:aws:s3:::amazonlinux-2-repos-region/*"
      ]
    }
  ]
}
```

Utiliser l'application Kernel Live Patching

Vous pouvez activer et utiliser Kernel Live Patching sur des instances individuelles à l'aide de la ligne de commande de l'instance elle-même, ou vous pouvez activer et utiliser Kernel Live Patching sur un groupe d'instances gérées à l'aide de AWS Systems Manager.

Les sections suivantes expliquent comment activer et utiliser Kernel Live Patching sur des instances individuelles à l'aide de la ligne de commande.

Pour plus d'informations sur l'activation et l'utilisation du Kernel Live Patching sur un groupe d'instances gérées, consultez la section Utiliser le Kernel Live Patching sur les AL2 instances dans le Guide de l'AWS Systems Manager utilisateur.

Rubriques

- Activer Kernel Live Patching
- Afficher les correctifs à chaud du noyau disponibles
- Appliquer des correctifs à chaud du noyau
- Afficher les correctifs à chaud du noyau appliqués
- Désactiver Kernel Live Patching

Activer Kernel Live Patching

Kernel Live Patching est désactivé par défaut sur AL2. Pour utiliser l'application Kernel Live Patching, vous devez installer le plug-in yum pour Kernel Live Patching et activer la fonctionnalité Kernel Live Patching.

Conditions préalables

Kernel Live Patching nécessite `binutils`. Si vous n'avez pas `binutils` installé, installez-le à l'aide de la commande suivante :

```
$ sudo yum install binutils
```

Pour activer Kernel Live Patching

1. Les correctifs dynamiques du noyau sont disponibles pour les versions de AL2 noyau suivantes :

   - Version `4.14` ou `5.10` du noyau sur l'architecture `x86_64`
   - Version `5.10` du noyau sur l'architecture `ARM64`

   Pour vérifier la version de votre noyau, exécutez la commande suivante.

   ```
   $ sudo yum list kernel
   ```
2. Si vous avez déjà une version du noyau prise en charge, ignorez cette étape. Si vous ne disposez pas d'une version du noyau prise en charge, exécutez les commandes suivantes pour mettre à jour le noyau vers la dernière version et pour redémarrer l'instance.

   ```
   $ sudo yum install -y kernel
   ```

   ```
   $ sudo reboot
   ```
3. Installez le plugin yum pour Kernel Live Patching.

   ```
   $ sudo yum install -y yum-plugin-kernel-livepatch
   ```
4. Activez le plugin yum pour Kernel Live Patching.

   ```
   $ sudo yum kernel-livepatch enable -y
   ```

Cette commande installe également la dernière version du RPM du correctif à chaud du noyau à partir des référentiels configurés.

5. Pour confirmer que le plugin yum pour Kernel Live Patching a bien été installé, exécutez la commande suivante.

```
$ rpm -qa | grep kernel-livepatch
```

Lorsque vous activez Kernel Live Patching, un RPM vide du correctif à chaud du noyau est automatiquement appliqué. Si Kernel Live Patching a été activé avec succès, cette commande renvoie une liste qui inclut le RPM vide initial du correctif à chaud du noyau. Voici un exemple de sortie.

```
yum-plugin-kernel-livepatch-1.0-0.11.amzn2.noarch
kernel-livepatch-5.10.102-99.473-1.0-0.amzn2.x86_64
```

6. Installez le package kpatch.

```
$ sudo yum install -y kpatch-runtime
```

7. Mettez à jour le service kpatch s'il a été installé précédemment.

```
$ sudo yum update kpatch-runtime
```

8. Démarrez le service kpatch. Ce service charge tous les correctifs à chaud du noyau lors de l'initialisation ou au démarrage.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

9. Activez la rubrique Kernel Live Patching dans la bibliothèque AL2 Extras. Cette rubrique contient les correctifs à chaud du noyau.

```
$ sudo amazon-linux-extras enable livepatch
```

Afficher les correctifs à chaud du noyau disponibles

Les alertes de sécurité Amazon Linux sont publiées dans le Centre de sécurité Amazon Linux. Pour plus d'informations sur les alertes AL2 de sécurité, qui incluent les alertes relatives aux correctifs

actifs du noyau, consultez le centre de sécurité Amazon Linux. Les correctifs Kernel Live sont préfixés avec `ALASLIVEPATCH`. Le Centre de sécurité Amazon Linux peut ne pas répertorier les correctifs à chaud du noyau qui corrigent les bogues.

Vous pouvez également découvrir les correctifs dynamiques du noyau disponibles pour les alertes et à CVEs l'aide de la ligne de commande.

Pour répertorier tous les correctifs à chaud du noyau disponibles pour les avis

Utilisez la commande suivante.

```
$ yum updateinfo list
```

Voici un exemple de sortie.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motd
ALAS2LIVEPATCH-2020-002 important/Sec. kernel-
livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
ALAS2LIVEPATCH-2020-005 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

Pour répertorier tous les correctifs dynamiques du noyau disponibles pour CVEs

Utilisez la commande suivante de l'.

```
$ yum updateinfo list cves
```

Voici un exemple de sortie.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motdamzn2-core/2/x86_64 | 2.4 kB 00:00:00
CVE-2019-15918 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2019-20096 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2020-8648 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

Appliquer des correctifs à chaud du noyau

Vous appliquez les correctifs à chaud du noyau en utilisant le gestionnaire de paquets yum de la même manière que vous appliquez les mises à jour régulières. Le plugin yum pour Kernel Live Patching gère les correctifs dynamiques du noyau qui peuvent être appliqués.

> **Tip**
>
> Nous vous recommandons de mettre régulièrement à jour votre noyau à l'aide de Kernel Live Patching afin de vous assurer qu'il reçoit des correctifs de sécurité spécifiques importants et critiques jusqu'à ce que le système puisse être redémarré. Vérifiez également si des correctifs supplémentaires ont été mis à disposition du package du noyau natif qui ne peuvent pas être déployés sous forme de correctifs actifs, puis mettez à jour et redémarrez la mise à jour du noyau dans ces cas.

Vous pouvez choisir d'appliquer un correctif à chaud du noyau spécifique ou d'appliquer tous les correctifs à chaud du noyau disponibles avec vos mises à jour de sécurité régulières.

Pour appliquer un correctif à chaud du noyau spécifique

1. Obtenez la version du correctif à chaud du noyau à l'aide de l'une des commandes décrites à la section Afficher les correctifs à chaud du noyau disponibles.
2. Appliquez le correctif dynamique du noyau pour votre AL2 noyau.

   ```
   $ sudo yum install kernel-livepatch-kernel_version.x86_64
   ```

   Par exemple, la commande suivante applique un correctif à chaud du noyau pour la version du noyau AL2 `5.10.102-99.473`.

   ```
   $ sudo yum install kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
   ```

Pour appliquer les correctifs à chaud du noyau disponibles avec vos mises à jour de sécurité régulières

Utilisez la commande suivante.

```
$ sudo yum update --security
```

Omettre l'option `--security`d'inclure les corrections de bogues.

> **Important**
>
> - La version du noyau n'est pas mise à jour après l'application des correctifs à chaud du noyau. La version est mise à jour vers la nouvelle version seulement après le redémarrage de l'instance.
> - Un AL2 noyau reçoit des correctifs dynamiques pendant une période de trois mois. Une fois la période de trois mois écoulée, aucun nouveau correctif à chaud du noyau n'est publié pour cette version du noyau. Pour continuer à recevoir les correctifs à chaud du noyau après la période de trois mois, vous devez redémarrer l'instance pour passer à la nouvelle version du noyau, qui continuera ensuite à recevoir les correctifs à chaud du noyau pendant les trois prochains mois. Pour vérifier la fenêtre de support de votre version du noyau, exécutez `yum kernel-livepatch supported`.

Afficher les correctifs à chaud du noyau appliqués

Pour afficher les correctifs à chaud du noyau appliqués

Utilisez la commande suivante.

```
$ kpatch list
```

La commande renvoie une liste des correctifs à chaud du noyau des mise à jour de sécurité chargés et installés. Voici un exemple de sortie.

```
Loaded patch modules:
livepatch_cifs_lease_buffer_len [enabled]
livepatch_CVE_2019_20096 [enabled]
livepatch_CVE_2020_8648 [enabled]

Installed patch modules:
livepatch_cifs_lease_buffer_len (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2019_20096 (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2020_8648 (5.10.102-99.473.amzn2.x86_64)
```

> **Note**
>
> Un seul correctif à chaud du noyau peut inclure et installer plusieurs correctifs à chaud.

Désactiver Kernel Live Patching

Si vous n'avez plus besoin d'utiliser Kernel Live Patching, vous pouvez le désactiver à tout moment.

Pour désactiver Kernel Live Patching

1. Supprimez les packages RPM pour les correctifs à chaud du noyau appliqués.

   ```
   $ sudo yum kernel-livepatch disable
   ```

2. Désinstallez le plugin yum pour Kernel Live Patching.

   ```
   $ sudo yum remove yum-plugin-kernel-livepatch
   ```

3. Redémarrez l'instance.

   ```
   $ sudo reboot
   ```

Limitations

Kernel Live Patching présente les limitations suivantes :

- Lorsque vous appliquez un correctif dynamique du noyau, vous ne pouvez pas effectuer d'hibernation, utiliser des outils de débogage avancés (tels que SystemTap des outils basés sur kprobes et EBPF) ou accéder aux fichiers de sortie ftrace utilisés par l'infrastructure Kernel Live Patching.
- > **Note**
  >
  > En raison de limitations techniques, certains problèmes ne peuvent pas être résolus par l'application de correctifs en direct. Pour cette raison, ces correctifs ne seront pas fournis dans le package de mise à jour dynamique du noyau, mais uniquement dans le package de mise à jour du package natif du noyau. Vous pouvez installer la mise à jour du package natif du noyau et redémarrer le système pour activer les correctifs comme d'habitude.

Questions fréquentes (FAQ)

Pour les questions fréquemment posées sur Kernel Live Patching for AL2, consultez la FAQ sur les correctifs Kernel Live d'Amazon Linux 2.

AL2 Bibliothèque d'extras

> **Warning**
>
> L'`epel`Extra active le EPEL7 référentiel tiers. Depuis le 30/06/2024, le EPEL7 référentiel tiers n'est plus maintenu.
> Ce référentiel tiers ne fera l'objet d'aucune future mise à jour. Cela signifie qu'il n'y aura aucun correctif de sécurité pour les packages dans le référentiel EPEL.
> Consultez la EPELsection du guide de l'utilisateur Amazon Linux 2023 pour connaître les options relatives à certains EPEL packages.

Avec AL2, vous pouvez utiliser la bibliothèque Extras pour installer des mises à jour d'applications et de logiciels sur vos instances. Ces mises à jour logicielles sont appelées rubriques. Vous pouvez installer une version spécifique d'une rubrique ou omettre les informations de version pour utiliser la version la plus récente. Les suppléments permettent d'éviter d'avoir à faire des compromis entre la stabilité d'un système d'exploitation et la fraîcheur des logiciels disponibles.

Le contenu des rubriques Extras est exempté de la politique d'Amazon Linux en matière de support à long terme et de compatibilité binaire. Les rubriques supplémentaires donnent accès à une liste organisée de packages. Les versions des packages peuvent être fréquemment mises à jour ou ne pas être prises en charge pendant la même durée que AL2.

> **Note**
>
> Les rubriques Extras individuelles peuvent être déconseillées avant d' AL2 atteindre leur date de fin de vie.

Pour répertorier les rubriques disponibles, utilisez la commande suivante.

```
[ec2-user ~]$ amazon-linux-extras list
```

Pour activer une rubrique et installer la dernière version de son package afin de garantir sa fraîcheur, utilisez la commande suivante.

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

Pour activer les rubriques et installer des versions spécifiques de leurs packages afin de garantir la stabilité, utilisez la commande suivante.

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

Pour supprimer un package installé à partir d'une rubrique, utilisez la commande suivante.

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk
 '{ print $1 }')
```

> **Note**
>
> Cette commande ne supprime pas les packages installés en tant que dépendances de l'Extra.

Pour désactiver un sujet et rendre les packages inaccessibles au gestionnaire de packages yum, utilisez la commande suivante.

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

> **Important**
>
> Cette commande est destinée aux utilisateurs avancés. Une utilisation incorrecte de cette commande peut entraîner des conflits de compatibilité de paquets.

Liste des extras d'Amazon Linux 2

Nom supplémentaire	Date déconseillée
BCC	
GraphicsMagick1.3	
R3,4	
R4	

Nom supplémentaire	Date déconseillée
ansible 2	30/09/2023
aws-nitro-enclaves-cli	
awscli1	
collectd	
collectd-python3	
corretto8	
dnsmasq	
dnsmasq2,85	01/05/2025
docker	
ecs	
emacs	2018-11-14
peler	30/06/2024
pétard	08/11/11
firefox	
gimp	2018-11-14
golang1,11	01/08/2023
golang1,19	30/09/2023
golang1,9	14/12/2018
haproxy2	
http_modules	

Nom supplémentaire	Date déconseillée
java-openjdk11	30/09/2024
kernel-5.10	
kernel-5.15	
noyau-5.4	
kernel-ng	08/08/2018
lamp-mariadb10.2-php7.2	2020-11-30
libreoffice	
LivePatch	
lustre	
lustre2.10	
lynis	
mariadb10,5	24/06/2025
mate-desktop1.x	
memcached1,5	
se moquer	
maquette 2	
mono	
nano	2018-11-14
nginx1	
nginx1.12	2019-09-20

Nom supplémentaire	Date déconseillée
nginx 1.22.1	
php7.1	15/01/2020
php7,2	2020-11-30
php7.3	2021-12-06
php7,4	03/11/11
php8.0	26/11/2023
php8.1	31/12/2025
php8.2	
postgresql10	30/09/2023
postgresql11	09/11/2023
postgresql12	14-11-2024
postgresql13	13/11/2025
postgresql14	
postgresql9.6	05.08-09
python3	22/08/2018
python3.8	14-10-2024
rouge 4.0	25/05/2021
redis6	31/01/2020
rubis 2,4	27/08/2020
rubis 2,6	31 avril

Nom supplémentaire	Date déconseillée
rubis 3.0	31/03/2024
rouille (1)	01/05/2025
sélinux−ng	
calmar (4)	30/09/2023
test	
tomcat8,5	31/03/2024
tomcat 9	
Unbound1,13	01/05/2025
Unbound1,17	
vim	2018-11-14

AL2 Utilisateurs et groupes réservés

AL2 préalloue certains utilisateurs et groupes à la fois lors du provisionnement de l'image et lors de l'installation de certains packages. Les utilisateurs, les groupes et leurs utilisateurs associés UIDs GIDs sont répertoriés ici pour éviter les conflits.

Rubriques

Liste des utilisateurs réservés d'Amazon Linux 2

Répertorié par UID

Nom utilisateur	UID
racine	0
bin	1
démon	2
adm	3
lp	4
sync	5
shutdown	6
arrêter	7
courrier	8
uucp	10
opérateur	11
jeux	12

Nom utilisateur	UID
ftp	14
profil	16
piuseur	17
calamar	23
nommé	25
postgres	26
mysql	27
nscd	28
nscd	28
utilisateur rpc	29
rpc	32
une sauvegarde	33
ntp	38
facteur	41
gdm	42
mailnull	47
apache	48
smmsp	51
tomcat	53
ldap	55

Nom utilisateur	UID
tss	59
nslcd	65
pegasus	66
avahi	70
tcpdump	72
sshd	74
radvd	75
cyrus	76
arpwatch	77
fax	78
dbus	81
postfix	89
quagga	92
radiusd	95
radiusd	95
hsqldb	96
pigeonnier	97
identifiant	98
personne	99
qemu	107

Nom utilisateur	UID
usbmuxd	113
serveur STAP	155
avahi-autoipd	170
pouls	171
rtkit	172
dhcpd	177
sanlock	179
haproxy	188
cluster	189
systemd-journal-gateway	191
réseau Systemd	192
systemd-resolve	193
uuidd	357
tang	358
stapdev	359
stapsys	360
stapurs	361
systemd-journal-upload	362
systemd-journal-remote	363
sablé	364

Nom utilisateur	UID
peigner	365
pcpqa	366
pcp	367
memcached	368
ipsilon	369
ipaapi	370
proxy kdc	371
cotes	372
sssd	373
gluster	374
fedfs	375
coquet de tourterelle	376
coroqnetd	377
chape	378
scan à palourdes	379
clamilt	380
mise à jour	381
colord	382
géoclue	383
aws-kinesis-agent-user	384

Nom utilisateur	UID
agent	385
non lié	386
poli	387
saslauth	388
dirsrv	389
chrony	996
ec2-instance-connect	997
rngd	998
libstoragemgmt	999
utilisateur ec2	1 000
nfsnobody	65534

Répertorié par nom

Nom utilisateur	UID
adm	3
une sauvegarde	33
apache	48
arpwatch	77
avahi	70
avahi-autoipd	170

Nom utilisateur	UID
aws-kinesis-agent-user	384
bin	1
chrony	996
clamilt	380
scan à palourdes	379
mise à jour	381
chape	378
colord	382
coroqnetd	377
agent	385
cyrus	76
démon	2
dbus	81
dhcpd	177
dirsrv	389
pigeonnier	97
govenull	376
ec2-instance-connect	997
utilisateur ec2	1 000
fax	78

Nom utilisateur	UID
fedfs	375
ftp	14
jeux	12
gdm	42
géoclue	383
gluster	374
cluster	189
arrêter	7
haproxy	188
hsqldb	96
identifiant	98
ipaapi	370
ipsilon	369
proxy kdc	371
ldap	55
libstoragemgmt	999
lp	4
courrier	8
facteur	41
mailnull	47

Nom utilisateur	UID
memcached	368
mysql	27
nommé	25
nfsnobody	65534
personne	99
nscd	28
nscd	28
nslcd	65
ntp	38
cotes	372
opérateur	11
oprofil	16
pcp	367
pcpqa	366
pegasus	66
peigner	365
piuseur	17
poli	387
postfix	89
postgres	26

Nom utilisateur	UID
pouls	171
qemu	107
quagga	92
radiusd	95
radiusd	95
radvd	75
rngd	998
racine	0
rpc	32
utilisateur rpc	29
rtkit	172
sablé	364
sanlock	179
saslauth	388
shutdown	6
smmsp	51
calamar	23
sshd	74
sssd	373
serveur STAP	155

Nom utilisateur	UID
stapdev	359
stapsys	360
stapurs	361
sync	5
systemd-journal-gateway	191
systemd-journal-remote	363
systemd-journal-upload	362
réseau Systemd	192
systemd-resolve	193
tang	358
tcpdump	72
tomcat	53
tss	59
non lié	386
usbmuxd	113
uucp	10
uuidd	357

Liste des groupes réservés Amazon Linux 2

Répertorié par GID

Nom du groupe	GID
racine	0
bin	1
démon	2
sys	3
adm	4
tty	5
disque	6
disque	6
lp	7
mem	8
kmem	9
roue	10
cdrom	11
courrier	12
uucp	14
man	15
oprofil	16
piuseur	17
dialout	18
flottant	19

Nom du groupe	GID
jeux	20
répartir	21
utmp	22
calamar	23
nommé	25
postgres	26
mysql	27
nscd	28
nscd	28
utilisateur rpc	29
rpc	32
ruban	33
ruban	33
tentateur	35
kvm	36
ntp	38
vidéos	39
tremper	40
facteur	41
gdm	42

Nom du groupe	GID
mailnull	47
apache	48
ftp	50
smmsp	51
tomcat	53
verrouiller	54
ldap	55
tss	59
audio	63
pegasus	65
avahi	70
tcpdump	72
sshd	74
radvd	75
saslauth	76
saslauth	76
arpwatch	77
fax	78
dbus	81
screen	84

Nom du groupe	GID
bourdon	85
wbpriv	88
wbpriv	88
postfix	89
post-dépôt	90
quagga	92
radiusd	95
radiusd	95
hsqldb	96
pigeonnier	97
identifiant	98
personne	99
users	100
qemu	107
usbmuxd	113
serveur STAP	155
stapurs	156
stapurs	156
stapsys	157
stapdev	158

Nom du groupe	GID
avahi-autoipd	170
pouls	171
rtkit	172
dhcpd	177
sanlock	179
haproxy	188
un client	189
journal Systemd	190
journal Systemd	190
systemd-journal-gateway	191
réseau Systemd	192
systemd-resolve	193
submon	351
wireshark	352
uuidd	353
tang	354
systemd-journal-upload	355
sfcb	356
systemd-journal-remote	356
sablé	357

Nom du groupe	GID
peigner	358
pcpqa	359
pcp	360
memcached	361
virtlogin	362
ipsilon	363
pkcs11	364
ipaapi	365
proxy kdc	366
cotes	367
sssd	368
libvirt	369
gluster	370
fedfs	371
coquet de tourterelle	372
docker	373
coroqnetd	374
chape	375
scan à palourdes	376
clamilt	377

Nom du groupe	GID
groupe de virus	378
groupe de virus	378
groupe de virus	378
mise à jour	379
colord	380
géoclue	381
admin d'impression	382
aws-kinesis-agent-user	383
agent	384
pulse-rt	385
accès par impulsion	386
non lié	387
poli	388
dirsrv	389
guéri	993
chrony	994
ec2-instance-connect	995
rngd	996
libstoragemgmt	997
clés SSH	998

Nom du groupe	GID
input	999
utilisateur ec2	1 000
nfsnobody	65534

Répertorié par nom

Nom du groupe	GID
adm	4
apache	48
arpwatch	77
audio	63
avahi	70
avahi-autoipd	170
aws-kinesis-agent-user	383
bin	1
cdrom	11
guéri	993
chrony	994
clamilt	377
scan à palourdes	376
mise à jour	379

Nom du groupe	GID
chape	375
colord	380
coroqnetd	374
agent	384
démon	2
dbus	81
dhcpd	177
boîte de dialogue	18
tremper	40
dirsrv	389
disque	6
disque	6
docker	373
pigeonnier	97
coquet de tourterelle	372
ec2-instance-connect	995
utilisateur ec2	1 000
fax	78
fedfs	371
flottant	19

Nom du groupe	GID
ftp	50
jeux	20
gdm	42
géoclue	381
gluster	370
un client	189
haproxy	188
hsqldb	96
identifiant	98
input	999
ipaapi	365
ipsilon	363
proxy kdc	366
kmem	9
kvm	36
ldap	55
libstoragemgmt	997
libvirt	369
verrouiller	54
lp	7

Nom du groupe	GID
courrier	12
facteur	41
mailnull	47
man	15
mem	8
memcached	361
mysql	27
nommé	25
nfsnobody	65534
personne	99
nscd	28
nscd	28
ntp	38
cotes	367
oprofil	16
pcp	360
pcpqa	359
pegasus	65
peigner	358
pkcs11	364

Nom du groupe	GID
piuseur	17
poli	388
post-dépôt	90
postfix	89
postgres	26
admin d'impression	382
pouls	171
accès par impulsion	386
pulse-rt	385
qemu	107
quagga	92
bourdon	85
radiusd	95
radiusd	95
radvd	75
rngd	996
racine	0
rpc	32
utilisateur rpc	29
rtkit	172

Nom du groupe	GID
sablé	357
sanlock	179
saslauth	76
saslauth	76
screen	84
sfcb	356
répartir	21
smmsp	51
calamar	23
clés SSH	998
sshd	74
sssd	368
serveur STAP	155
stapdev	158
stapsys	157
stapurs	156
stapurs	156
sys	3
journal Systemd	190
journal Systemd	190

Nom du groupe	GID
systemd-journal-gateway	191
systemd-journal-remote	356
systemd-journal-upload	355
réseau Systemd	192
systemd-resolve	193
tang	354
ruban	33
ruban	33
tcpdump	72
tomcat	53
tss	59
tty	5
non lié	387
submon	351
usbmuxd	113
users	100
tentateur	35
utmp	22
uucp	14
uuidd	353

Nom du groupe	GID
vidéos	39
virtlogin	362
groupe de virus	378
groupe de virus	378
groupe de virus	378
wbpriv	88
wbpriv	88
roue	10
wireshark	352

AL2 Paquets source

Vous pouvez voir la source des packages que vous avez installés sur votre instance à des fins de référence en utilisant des outils fournis dans Amazon Linux. Les packages source sont disponibles pour tous les packages compris dans Amazon Linux et le référentiel de package en ligne. Déterminez le nom du package source que vous souhaitez installer et utilisez la yumdownloader --source commande pour afficher le code source dans votre instance en cours d'exécution. Par exemple :

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

Le RPM source peut être décompressé et, à titre de référence, vous pouvez consulter l'arborescence des sources à l'aide des outils RPM standard. Après le débogage, le package peut être utilisé.

Sécurité et conformité dans AL2

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWSvous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWSconformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AL2 023, voir AWSServices concernés par programme de conformité AWS .
- Sécurité dans le cloud : votre responsabilité est déterminée par le AWSservice que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Activer le mode FIPS sur AL2

Cette section explique comment activer les normes fédérales de traitement de l'information (FIPS) sur AL2. Pour plus d'informations sur FIPS, consultez les références suivantes :

- Norme FIPS (Federal Information Processing Standard)
- Conformité FAQs : normes fédérales de traitement de l'information

Conditions préalables

- Une EC2 instance AL2 Amazon existante avec accès à Internet pour télécharger les packages requis. Pour plus d'informations sur le lancement d'une EC2 instance AL2 Amazon, consultezAL2 sur Amazon EC2.
- Vous devez vous connecter à votre EC2 instance Amazon via SSH ouAWS Systems Manager.

> **Important**
>
> ED25519 Les clés utilisateur SSH ne sont pas prises en charge en mode FIPS. Si vous avez lancé votre EC2 instance Amazon à l'aide d'une paire de clés ED25519 SSH, vous devez générer de nouvelles clés à l'aide d'un autre algorithme (tel que RSA) ou vous risquez de perdre l'accès à votre instance après avoir activé le mode FIPS. Pour plus d'informations, consultez la section Créer des paires de clés dans le guide de EC2 l'utilisateur Amazon.

Activation du mode FIPS

1. Connectez-vous à votre AL2 instance via SSH ouAWS Systems Manager.
2. Assurez-vous que le système est à jour. Pour de plus amples informations, veuillez consulter Référentiel de packages.
3. Installez et activez le `dracut-fips` module en exécutant les commandes suivantes.

   ```
   sudo yum -y install dracut-fips
   sudo dracut -f
   ```

4. Activez le mode FIPS sur la ligne de commande du noyau Linux à l'aide de la commande suivante. Cela permettra d'activer le mode FIPS à l'échelle du système pour les modules répertoriés dans la FAQ AL2

   ```
   sudo /sbin/grubby --update-kernel=ALL --args="fips=1"
   ```

5. Redémarrez votre AL2 instance.

   ```
   sudo reboot
   ```

6. Pour vérifier que le mode FIPS est activé, reconnectez-vous à l'instance et exécutez la commande suivante.

   ```
   sysctl crypto.fips_enabled
   ```

   Vous devriez voir la sortie suivante :

   ```
   crypto.fips_enabled = 1
   ```

Vous pouvez également vérifier qu'OpenSSH est en mode FIPS en exécutant la commande suivante :

```
ssh localhost 2>&1 | grep FIPS
```

Vous devriez voir la sortie suivante :

```
FIPS mode initialized
```

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.