



Amazon Linux AMI User Guide

Last Updated: March 15, 2011

This document is an overview of key technologies in the Amazon Linux AMI. It covers adding and building packages, the product life cycle, how to get support, and a brief FAQ. This document assumes general knowledge of Linux system administration, Amazon Elastic Compute Cloud, and instance launch and management.

Introduction

The Amazon Linux AMI is a supported and maintained Linux image provided by Amazon Web Services (AWS) for use on Amazon Elastic Compute Cloud (Amazon EC2). It is designed to provide a stable, secure, and high-performance execution environment for applications running on Amazon EC2. It also includes several packages that enable easy integration with AWS, including launch configuration tools and many popular AWS libraries and tools. Amazon Web Services also provides ongoing security and maintenance updates to all instances running the Amazon Linux AMI. The Amazon Linux AMI is provided at no additional charge to Amazon EC2 users.

Finding the AMI

Visit <http://aws.amazon.com/amazon-linux-ami> for the latest list of AMI IDs to launch.

Logging In

To prevent remote root exploits, the Amazon Linux AMI does not allow remote root login via SSH. Also, password authentication is disabled to prevent brute-force password attacks. To enable SSH logins to a running Amazon Linux AMI, you must provide your key pair to the instance at launch. You must also set the security group used to launch your instance to allow SSH access. By default, the only account that can log in remotely via SSH is ec2-user. The ec2-user has sudo privileges.

The AWS Management Console provides a web user interface for performing the same actions. You can read more information at <http://aws.amazon.com/console/>.

Identifying Images

Each image contains a unique /etc/image-id that identifies the AMI. This file contains information about the image. Here is an example /etc/image-id file:

```
# cat /etc/image-id
image_name="amzn-ami"
image_version="2011.02.1"
image_arch="x86_64"
image_file="amzn-ami-2011.02.1.x86_64.ext4"
```



```
image_stamp="9f15-0657"  
image_date="20110224163136"  
recipe_name="amzn ami"  
recipe_id="157fed54-3193-49e1-8ac4-53595517377f"
```

The `image_name`, `image_version`, and `image_arch` items come from the build recipe that Amazon used to construct the image. The `image_stamp` is simply a unique random hex value generated during image creation. The `image_date` item is in `YYYYMMDDhhmmss` format, and is the UTC time of image creation. The `recipe_name` and `recipe_id` refer to the name and ID of the build recipe Amazon used to construct the image, which identifies the current running version of the Amazon Linux AMI. This file will change as you install updates from the yum repository.

Included AWS Command Line Tools

The following popular command line tools for AWS integration and usage have been included in the Amazon Linux AMI:

- `aws-apitools-common`
- `aws-apitools-mon`
- `aws-apitools-ec2`
- `aws-apitools-elb`
- `aws-apitools-rds`
- `aws-apitools-as`
- `aws-apitools-iam`
- `aws-scripts-ses`

To simplify the configuration of these tools, a simple script has been included to prepare `AWS_CREDENTIAL_FILE`, `JAVA_HOME`, `AWS_PATH`, `PATH`, and product-specific environment variables after a credential file has been installed.

Also, to allow the installation of multiple versions of the API and AMI tools, we have placed symlinks to the desired versions of these tools in `/opt/aws`, as described here:

- `/opt/aws/bin`—Symlink farm to `/bin` directories in each of the installed tools directories.
- `/opt/aws/{apitools|amitools}`—Products are installed in directories of the form `[name]-version` and symlink `[name]` attached to the most recently installed version.
- `/opt/aws/{apitools|amitools}/[name]/environment.sh`—Used by `/etc/profile.d/aws-apitools-common.sh` to set product-specific environment variables (`EC2_HOME`, etc.).

Cloud-init

Cloud-init is an open source application built by Canonical that is used to bootstrap Linux images in a cloud computing environment such as Amazon EC2. The Amazon Linux AMI contains a version of Cloud-init. It enables you to specify actions that should happen to your instance at boot time. You can pass desired actions to Cloud-init through the user data fields when launching an instance. This means you can use a common AMI for many use cases and configure them dynamically at startup. The Amazon Linux AMI also uses Cloud-init to perform initial configuration of the `ec2-user` account.

For more information about Cloud-init, see <https://help.ubuntu.com/community/CloudInit>.



The Amazon Linux AMIs use the following Cloud-init features (configurable in /etc/sysconfig/cloudinit):

- **action:** INIT (always runs)
 - Setting a default locale.
 - Setting the hostname.
 - Parsing and handling user-data.
- **action:** CONFIG_SSH
 - Generating host private SSHkeys.
 - Adding user's public SSHkeys to .ssh/authorized_keys for easy login and administration.
- **action:** PACKAGE_SETUP
 - Preparing yum repo.
 - Handles package actions defined in user-data (see cloud-config syntax).
- **action:** RUNCMD
 - Runs a shell command (see cloud-config syntax).
- **action:** RUN_USER_SCRIPTS
 - Executes user scripts found in user-data (see formats section).
- **action:** CONFIG_MOUNTS
 - Mounts ephemeral drives.

Supported User-data formats

Cloud-init supports user-data handling of a variety of formats:

- **Gzip**
 - If user-data is gzip compressed, Cloud-init will decompress the data and handle as appropriate.
- **MIME multipart**
 - Using a mime-multi part file enables the user to specify more than one type of data. For example, both a user-data script and a cloud-config type could be specified. Each part of the multi-part file may be handled by Cloud-init if it is one of the supported formats.
- **Base64 decoding**
 - If user-data is base64 encoded, Cloud-init will determine if it can understand the decoded data as one of the supported types. If it understands the decoded data, it will decode the data and handle as appropriate. If not, it will return the base64 data intact.
- **User-Data Script**
 - Begins with "#!" or "Content-Type: text/x-shellscrip".
 - The script will be executed by "/etc/init.d/Cloud-init-user-scripts" level during first boot. This occurs late in the boot process (after the initial configuration actions were performed).
- **Include File**
 - Begins with "#include" or "Content-Type: text/x-include-url".
 - This content is an "include" file. The file contains a list of URLs, one per line. Each of the URLs will be read, and their content will be passed through this same set of rules; i.e., the content read from the URL can be gzipped, mime-multi-part, or plain text.
- **Cloud Config Data**
 - Begins with "#cloud-config" or "Content-Type: text/cloud-config".
 - This content is "cloud-config" data. See the examples for a commented example of supported config formats.



- **Cloud Boothook**

- Begins with "#cloud-boothook" or "Content-Type: text/cloud-boothook".
- This content is "boothook" data. It is stored in a file under /var/lib/cloud and then executed immediately.
- This is the earliest "hook" available. Note that there is no mechanism provided for running only once. The boothook must take care of this itself. It is provided with the instance ID in the environment variable "INSTANCE_ID". This could be made use of to provide a "once-per-instance".

Adding Packages

In addition to the packages included in the Amazon Linux AMI, Amazon provides a yum repository of additional common Linux applications for use inside of Amazon EC2. The Amazon Linux AMI is configured to point to this repository by default for all yum actions. The packages can be installed by issuing yum commands. For example:

```
# sudo yum install httpd
```

The packages available from the Amazon Linux AMI yum repository in Amazon EC2 are designed to work with the Amazon Linux AMI. In addition, the Amazon Linux AMI has been built to be binary-compatible with the CentOS series of releases, and therefore packages built to run on CentOS should also run on the Amazon Linux AMI.

Important: Instances running in an Amazon Virtual Private Cloud (VPC) need to have an Internet Gateway attached to the VPC to contact the yum repository. For information, see

http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPCInternet_Gateway.html.

Accessing Source Packages for Reference

You can view source packages inside Amazon EC2 for reference purposes by using tools provided in the Amazon Linux AMI. Source packages are available for all of the packages included in the Amazon Linux AMI and the online package repository. Simply determine the package name for the source package you want to install and use the get_reference_source command to view source within your running instance. For example:

```
#get_reference_source -p httpd
Please enter your AWS account id: 123456789012

Requested package: httpd
Found package from local RPM database: httpd-2.2.15-2.9.amzn1
Corresponding source RPM to found package : httpd-2.2.15-2.9.amzn1.src.rpm
Your AWS account id: 123456789012

Are these parameters correct? Please type 'yes' to continue: yes
Source RPM downloaded to: /usr/src/srpm/debug/httpd-2.2.15-2.9.amzn1.src.rpm
```

You will need to enter your AWS account ID once you run the command. The source RPM will be placed in the /usr/src/srpm/debug directory of your running Amazon EC2 instance. From there it can be unpacked and for reference you can view the source tree using standard RPM tools. After you finish debugging, the package will be available for use in Amazon EC2.



Important: Instances running in an Amazon Virtual Private Cloud (VPC) need to have an Internet Gateway attached to the VPC to contact the yum repository. For information, see http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html.

Developing Applications

A full set of Linux development tools is provided in the yum repository for the Amazon Linux AMI. To develop applications on the Amazon Linux AMI, simply select the development tools you need with yum. Alternatively, many applications developed on CentOS and other similar distributions should run on the Amazon Linux AMI.

Ephemeral Store Access

The ephemeral drive ephemeral0 is mounted in /media/ephemeral0 only on Amazon Simple Storage Services (Amazon S3) backed AMIs. This is different than many other images that mount the ephemeral drive under /mnt.

Product Life Cycle

Customers can get started by launching the latest Amazon Linux AMI in Amazon EC2. The Amazon Linux AMI will be updated regularly with security and feature enhancements. Customers who do not need to preserve data or customizations on their running Amazon Linux AMI instances can simply relaunch new instances with the latest updated Amazon Linux AMI. Customers who do need to preserve data or customizations on their running Amazon Linux AMI instances can maintain those instances through the Amazon Linux AMI yum repositories. As the Amazon Linux AMI is updated, all of the updated packages will also be provided through these repositories and customers can chose to apply these updates to their running instances. Older versions of the AMI and update packages will continue to be available for launch in Amazon EC2 and for installation from the Amazon Linux AMI yum repository, even as new Amazon Linux AMI versions are released. However, in some cases, customers seeking support for an older version of the Amazon Linux AMI through Amazon Premium Support may be asked to move to newer versions as part of the support process.

Important: Instances running in an Amazon Virtual Private Cloud (VPC) need to have an Internet Gateway attached to the VPC to contact the yum repository. For information, see http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html.

Security Updates

Security updates are provided via the Amazon Linux AMI yum repositories and updated Amazon Linux AMIs. Major security alerts will be published in the AWS Security Center. For more information on AWS security policies or to report a security problem, visit the AWS Security Center at <http://aws.amazon.com/security/>.

Amazon Linux AMI is configured to download and install security updates at launch time. This is controlled via a Cloud-init setting called repo_upgrade. The following snippet of Cloud-init configuration shows how you can change the settings in the user data text you pass to your instance initialization:

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

The possible values for the repo_upgrade setting are as follows:

- **security**
 - Apply outstanding updates that Amazon marks as security updates.



- **bugfix**
 - Apply updates that Amazon marks as bug fixes. Bug fixes are a larger set of updates, which include security updates and fixes for various other minor bugs.
- **all**
 - Apply all applicable available updates, regardless of their classification.
- **none**
 - Do not apply any updates to the instance on startup.

The default setting for `repo_upgrade` is `security`. That is, if you don't specify a different value in your user data, by default the Amazon Linux AMI will perform the security upgrades for any applicable packages in your instance. Updates are applied only for those packages that you have installed on your instance at the time the check is performed.

Important: Instances running in an Amazon Virtual Private Cloud (VPC) need to have an Internet Gateway attached to the VPC to contact the yum repository. For information, see http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html.

Support

Support for installation and use of the base Amazon Linux AMI is included through subscriptions to AWS Premium Support. For more information on Premium Support, visit <http://aws.amazon.com/premiumsupport/>.

You're encouraged to post any questions you have on using the Amazon Linux AMI to the Amazon EC2 forums at <http://developer.amazonwebservices.com/connect/forum.jspa?forumID=30&start=0>.

You can report bugs either to Premium Support or the Amazon EC2 forums.

Frequently Asked Questions

Is the Amazon Linux AMI compatible with other Linux distributions?

The Amazon Linux AMI is very similar to CentOS in file system layout and package management. Applications built for CentOS 5 and later should run without recompilation of the Amazon Linux AMI. However, the Amazon Linux AMI is configured for use only in Amazon EC2.

How do I get root SSH access on my Amazon Linux AMI instance?

The Amazon Linux AMI does not allow remote root SSH by default. You should specify a key pair at instance launch and login as `ec2-user` using your key pair to access the command line. This user has `sudo` access by default to allow you to run root actions. If you want to enable remote root login, please be aware that it is significantly less secure than relying on key pairs and a secondary user.

How do I get my application on my Amazon Linux AMI instance?

Just as you would with any image you boot in Amazon EC2 today. You simply upload your application directly to your instance (such as with `scp`) and log in directly to the system to configure and launch it. Alternatively, you can pass commands to your instance at start up via the `user-data` field when you launch and use the built in Cloud-init package to parse the commands.

Which applications are part of the Amazon Linux AMI?

The Amazon Linux AMI was designed to be small by default. It lets you add additional applications from our online package repository. For example, the base image contains Python and Perl, while Apache HTTP Server, PHP, MySQL,



PostgreSQL, and many others are found on the repository server. The base image also contains all tools and libraries to integrate with other AWS products.

Does the Amazon Linux AMI support third-party independent software vendor (ISV) applications?

Yes. Most ISV applications that are designed to run on CentOS 5 or later will run on the Amazon Linux AMI. However, the Amazon Linux AMI has not gone through any formal certification efforts with ISVs. If you have a specific question about whether an ISV will officially support running its application on the Amazon Linux AMI, please contact the ISV directly.

What if I need an application the Amazon Linux AMI doesn't offer?

If you find that the Amazon Linux AMI does not contain an application you need, you can simply install the application directly on your Amazon Linux AMI instance just as you would any image today. The Amazon Linux AMI uses RPM and yum for package management and that will likely be the simplest way to install new applications. You should always check to see if an application is available in our central Amazon Linux AMI repository first because many apps are available there. These apps can easily be added to your AMI instance.

Does Amazon offer phone or web support services for the Amazon Linux AMI?

Yes. Amazon customers with Premium Support can use the standard support mechanisms to resolve issues regarding launching and general usage of the Amazon Linux AMI. Support covers the installation and use of the base Amazon Linux AMI, and the installation of additional packages from the Amazon Linux repository. Regardless of whether you enroll in Premium Support, you can access the AWS forums to report issues or request assistance from the AWS community.

How frequently is the Amazon Linux AMI updated?

Feature updates will typically be released no more than every 6 months and no less than every 12 months. Security updates will be released as required. Amazon will endeavor to provide updates with minimal impact on client applications and will notify users when an update is expected to have a negative impact on client applications.

Will Amazon release updates for all previous versions or only the most recent version?

Amazon Linux AMI updates are officially released and supported for the most recent version only. However, if you're running older versions of the Amazon Linux AMI, you can selectively apply updates from future versions using the command line or update API.

Can I run Amazon Linux on my own servers outside of Amazon EC2?

No. The Amazon Linux AMI is provided only inside of Amazon EC2.

Is the Amazon Linux AMI available in Amazon EC2 Virtual Private Cloud (VPC)?

Yes.

Important: Instances running in an Amazon Virtual Private Cloud (VPC) need to have an Internet Gateway attached to the VPC to contact the yum repository. For information, see

http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html.

Is a software development environment provided in the Amazon Linux AMI?

Yes. Complete development libraries and tools are incorporated in the Amazon Linux AMI so that you can develop applications directly on the Amazon Linux AMI.

Is there an Amazon Linux AMI community I can become a part of?

Yes. We encourage you to post your suggestions and feedback in the Amazon EC2 forum pages, which you can find at <http://developer.amazonwebservices.com/connect/forum.jspa?forumID=30>.