AWS Management Portal for vCenter

User Guide

aws

AWS Management Portal for vCenter: User Guide

Table of Contents

What Is AWS Management Portal for vCenter?

AWS Management Portal for vCenter provides a simple, easy-to-use interface for creating and managing AWS resources from VMware vCenter. For more information, see AWS Management Portal for vCenter.

> **Note**
> We recommend using AWS Server Migration Service (SMS) to migrate VMs from a vCenter environment to AWS. SMS automates the migration process by replicating on-premises VMs incrementally and converting them to Amazon machine images (AMIs). You can continue using your on-premises VMs while migration is in progress. For more information about AWS SMS, see AWS Server Migration Service.

Usage

- Administrators manage AWS networks, organize AWS resources using environments, and grant permissions to users at the environment level.
- Users can view the instances in the environments that they have permission to read, and create and manage EC2 instances in the environments that they have permission to modify.
- Users can import their virtual machines to AWS using the AWS Connector for vCenter.

Limitations

- You can connect each vCenter with one AWS account and one authentication provider.
- Users can't access the management portal unless they have an account that they can use to log in to vCenter. When users log in to vCenter and open the management portal, they can see environments, and AWS resources created in that environment, only if an administrator granted them permissions to access the environment. An administrator can grant users permissions only if their domain and user names meet certain requirements. Domain and user names are case-sensitive. If a user is a domain user, *domain\user* must not exceed 32 characters. If a user is a local user, *user* must not exceed 32 characters. The *domain* and *user* values must each begin with a letter and contain only the following characters: a-z, A-Z, 0-9, periods (.), underscores (_), and dashes (-).
- The management portal primarily supports Amazon EC2 resources. Future releases might support resources for additional services.
- You can't launch EC2 instances into EC2-Classic; you must launch instances into a VPC.
- This is not a comprehensive tool for creating and managing AWS resources. The management portal enables vCenter users to get started quickly with basic tasks, such as creating a VPC and subnet, and launching an EC2 instance. To complete more advanced tasks, users must use the AWS Management Console, AWS CLI, or an AWS SDK. For more information, see Accessing Amazon EC2 in the *Amazon EC2 User Guide*.

Requirements

- An AWS account

- vCenter version 5.1, 5.5, or 6.0. (Web client is supported on vCenter 5.5 and 6.0 only).

- Internet Explorer version 10

- Internet Explorer is set to allow cookies

- Network connectivity:
  - DHCP: Allow the connector to reach the DHCP server.
  - DNS: Allow the connector to initiate connections to port 53 for name resolution. Ensure that your firewall is stateful for these connections.
  - HTTPS outgoing: Allow the connector to initiate connections on port 443. Ensure that your firewall is stateful for these connections.
  - ICMP outgoing: Allow the connector outgoing connections using ICMP.
  - NTP: Allow the connector to initiate connections to port 123 to synchronize the time with the NTP servers. Ensure that your firewall is stateful for these connections.

How to Get Started

AWS Management Portal for vCenter User Guide
Installing and Configuring AWS
Management Portal for vCenter

Setting Up AWS Management Portal for vCenter

When you set up the management portal, you enable users in your organization to access your AWS resources. The process involves creating accounts, setting up trust between the management portal and your authentication provider, and deploying and configuring the connector.

To set up the management portal, complete the following tasks:

Tasks

> **Note**
> We recommend using AWS Server Migration Service (SMS) to migrate VMs from a vCenter environment to AWS. SMS automates the migration process by replicating on-premises VMs incrementally and converting them to Amazon machine images (AMIs). You can continue using your on-premises VMs while migration is in progress. For more information about AWS SMS, see AWS Server Migration Service.

Installing and Configuring AWS Management Portal for vCenter

You can choose one of two authentication providers: the AWS Connector for vCenter or an identity provider (IdP) that supports SAML 2.0. The setup process for the management portal differs based on the authentication provider that you choose. The following table describes your options. Follow the directions for the authentication provider that you chose.

Authentication Provider	Description
Federation authentication proxy (p. 5)	You can configure the connector to authenticate users. There are no prerequisites for this option. As part of the setup process, you'll set up a trust relationship between the management portal and the connector. This option is provided for organizations that aren't using an IdP that supports SAML 2.0.
SAML-based authentication (p. 10)	SAML 2.0 provides an open standard specifically designed for single sign-on (SSO). This enables users who have been authenticated by your IdP to access the management portal. To use this option, you must first set up an IdP for your organization. As part of the setup process, you'll

Authentication Provider	Description
	set up a SAML provider and configure a trust relationship between the management portal and AWS.
	For more information about the benefits of SAML, see Advantages of SAML.

After you select an authentication provider, complete the setup process. To select a different authentication provider, return to the first page of the setup program and then click **Reset Trust Relationship**, or expand **Reset Trust Relationship** on the summary page, click **I acknowledge that I want to reset my trust relationships configuration**, and then click **Reset Trust Relationship**.

Configuring Time Synchronization

The connector virtual appliance synchronizes its time with the time of its ESX/ESXi server. The connector requires that the Network Time Protocol (NTP) is configured on the ESXi server where it is deployed.

If the setup program fails to register your credentials, it's possible that this is a time synchronization issue. To verify, open `debug-file.log` and search for the following string: **ntpdate, -qv, pool.ntp.org**. If the offset is greater than 15 seconds, configure NTP on the ESX/ESXi server and restart the connector.

(Optional) Configuring Network Settings

You can configure various network settings using the connector command line interface (CLI).

To update your network settings using the connector CLI

1. Locate the connector VM in the vSphere client, right-click it, and select **Open Console.**
2. Log in as **ec2-user** with the password **ec2pass**.
3. Run the **sudo setup.rb** command. This command displays the following menu:

```
Choose one of the following options
1. Reset password
2. Reconfigure network settings
3. Restart services
4. Factory reset
5. Delete unused upgrade-related files
6. Enable/disable SSL certificate validation
7. Display connector's SSL certificate
8. Generate log bundle
9. Exit
Please enter your option [1-9]:
```

4. Type 2, and then press Enter. The command displays the following menu:

```
Reconfigure your network:
1. Renew or acquire a DHCP lease
2. Set up a static IP
3. Set up a web proxy for AWS communication
4. Set up a DNS suffix search list
5. Exit
```

```
Please enter your option [1-5]:
```

Use these options to complete the following tasks:

1. Renew your DHCP lease, or re-enable DHCP after setting up a static IP address.
2. Set up a static IP address for the connector. When prompted, enter the static IP address, netmask, gateway, and DNS servers.
3. Configure the connector to use a corporate web proxy. When prompted, enter the proxy IP address, port, and an optional user name and password to log in to the proxy. If you need to use authentication for the web proxy, note that the connector supports only password-based authentication.

   Note
   This option requires that you've set your initial password by logging into the connector using https://*ip_address*/, where *ip_address* is the IP address of the connector management console

4. Configure the DNS suffix search list so that connector can migrate VMs from the ESX host. You do not need to do this if vCenter displays all ESX hosts using fully-qualified domain names or IP addresses.
5. If the IP address changes or the proxy settings change, re-register the connector as follows:

   a. Using a web browser, open the connector management console.
   b. From the dashboard, click **Register the Connector**.
   c. Follow the directions to complete the registration wizard.

Option 1: Federation Authentication Proxy

You can set up the management portal to authenticate users using the AWS Connector for vCenter.

Your users don't have direct access to AWS resources. Instead, the vSphere client gets the user's information from your vCenter server and assumes an AWS Identity and Access Management (IAM) role to get temporary AWS security credentials for the user. The following diagram illustrates this process.
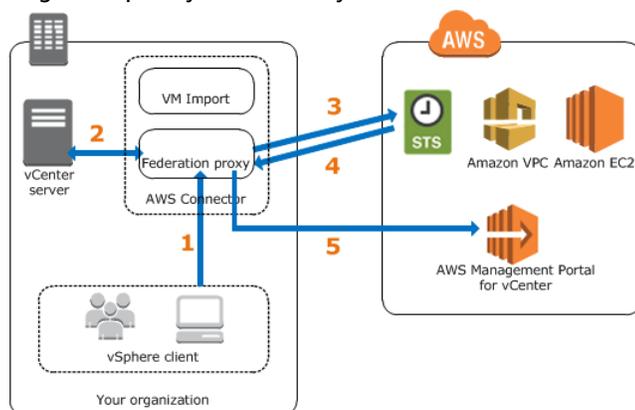
Federation authentication proxy

1. The user signs in to vCenter, clicks **Home**, and then clicks **AWS Management Portal**. The vSphere client sends an authentication request to the connector.
2. The connector authenticates the user.
3. The connector requests temporary security credentials from AWS Security Token Service (AWS STS).
4. AWS STS sends the connector temporary security credentials for the user.

5. Users are granted access to AWS resources based on the permissions assigned to them by an administrator.

Tasks

To set up the management portal, complete the following tasks:

Creating the Required Accounts and Users

First, create the accounts and users that are required by the management portal.

To create the required accounts and users

1. If your organization doesn't have an AWS account already, use the following steps to create one:

   a. Open https://portal.aws.amazon.com/billing/signup.

   b. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   You can complete the setup process using the credentials of either your AWS account or an IAM user. For more information about AWS Identity and Access Management (IAM), see *IAM User Guide*. To allow an IAM user to set up the management portal, you must grant that user permission to use the actions specified in the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:*",
                "amp:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::export-to-s3-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```

2. Create the *AWS authenticator provider account*, which is an IAM user that the connector uses to assume a trust role and authenticate users.

    a. Open the IAM console at https://console.aws.amazon.com/iam/.

    b. In the navigation pane, click **Users**.

    c. Click **Add user**.

    d. On the **Add user** page, type a user name, select **Programmatic access**, and then click **Next: Permissions**.

    e. Select **Attach existing policies directly**.

    f. In the search field, type `AWSConnector`. Select the checkbox for the **AWSConnector** policy and then click **Next: Review**.

    g. Click **Create user**.

    h. Save the credentials for this account in a safe location and then click **Close**.

        Important
        You'll need these credentials to complete the connector setup process.

3. Create the *vCenter service account*, which is a local or domain user that the connector uses to communicate with vCenter. Specify a unique, random password for the account. Do not manually assign vCenter privileges to this user at this point. We assign the vApp Export privilege to this user during the connector setup process. Note that you can restrict this privilege to specific parts of your vCenter inventory after you complete the connector setup process.

    Important
    Save the credentials for this account in a safe location. You'll need them to complete the connector setup process.

You can create this user using your IdP, vCenter, or Windows; whichever is easiest for you. For more information about creating local or domain users, see the following documentation, or contact an administrator for your vCenter or your IdP:

- Active Directory: Create a New User Account
- Windows: Create a local user account
- vCenter 5.5: Add vCenter Single Sign-On Users (the default domain is `vsphere.local`)
- vCenter 5.1: Add a vCenter Single Sign On User (the default domain is `System-Domain`)
- vCenter Server Appliance: Create a Local User Account in the vCenter Server Appliance

Setting Up the Trust Relationship

Complete the following procedure to set up a trust relationship between the management portal and the connector.

To set up the trust relationship

1. Open the AWS Management Portal for vCenter setup console.

    Tip
    If you've already completed the setup process but would like to change authentication providers, go to the summary page, expand **Reset Trust Relationship**, click **I acknowledge that I want to reset my trust relationships configuration**, and then click **Reset Trust Relationship**.

2. Click **Get started now**.

3. On the **AWS Management Portal for vCenter Configuration** page, select **AWS Connector** as the authentication provider.

4. On the **Configure the Trust Relationship** page, do one of the following:

   Option 1: Set up trust

   a. Specify the name of the IAM user that you created as the AWS authenticator provider account.

   b. (Optional) Review the policies for the AMP trust role, AMP service role, and import service role.

   c. Select **I agree that AWS Management Portal for vCenter may create the above roles on my behalf**.

   d. Click **Save and Continue**.

   Option 2: Change authentication providers

   If you previously selected **SAML-based authentication provider** as the authentication provider, click **Reset Trust Relationship**. After the reset, you can start the setup process again, select **AWS Connector**, and then set up trust.

5. On the **Add Administrators** page, add one to five users from your organization as administrators of the management portal, and then click **Save and Continue**. Note that you can specify both local and domain users.

   > **Important**
   > Domain and user names are case-sensitive.

   Use the form *domain\user*, where *domain* is optional for local users. For domain users, *domain\user* must not exceed 32 characters. For local users, *user* must not exceed 32 characters. The *domain* and *user* names must each begin with a letter and contain only the following characters: a-z, A-Z, 0-9, periods (.), underscores (_), and dashes (-).

   Note that you must add at least one administrator now, but you can add additional users as administrators later on. For more information, see Managing Administrators (p. 23).

6. On the **Create an AMP Connector Key** page, enter the name for the AMP connector key, and then click **Create**.

7. On the **Review Your Configuration** page, click **Download Configuration**, which downloads a file that contains your trust relationship configuration. Save this file to a safe location; you'll need it to complete the connector deployment process. Click **Finish**.

   Note that you can create a new AMP trust role or AMP connector key if you believe they were compromised.

8. On the **AWS Management Portal Setup** page, you can review and edit your current setup configuration.

Deploying the Connector Virtual Appliance

The management portal requires that you deploy and configure the connector, which manages the administrators and permissions.

The connector is packaged as a virtual appliance. To deploy the connector, complete the following procedure.

To deploy the Connector virtual appliance

1. Sign in to vCenter as a VMware administrator.

2. From the **File** menu, click **Deploy OVF Template**. Enter the following URL into the **Deploy from a file or URL** field and then click **Next**:

```
https://s3.amazonaws.com/aws-connector/AWS-Connector.ova
```

(Optional) To verify the download, use the following MD5 and SHA256 checksums:

```
https://s3.amazonaws.com/aws-connector/AWS-Connector.ova.md5sum
https://s3.amazonaws.com/aws-connector/AWS-Connector.ova.sha256sum
```

3. Complete the wizard. On the **Disk Format** page, select one of the thick provision disk types. We recommend that you select **Thick Provision Eager Zeroed**, as it has the best performance and reliability; however, it requires several hours to zero the disk. Do not select **Thin Provision**; this option makes deployment faster but significantly reduces disk performance. For more information, see Types of supported virtual disks in the VMware documentation.

4. Locate the newly deployed template in the vSphere client inventory tree, right-click it, and select **Power > Power On**. Right-click the template again and select **Open Console**. The console displays the IP address of the connector management console. Save the IP address in a secure location; you'll need it to complete the connector setup process.

> **Note**
> If you don't have a DHCP server, you must configure a static IP address. For more information, see (Optional) Configuring Network Settings (p. 4).

Configuring the Connector

To complete the setup process, open a web browser and complete the following procedure.

To configure the connector using the connector management console

1. From your web browser, go to https://*ip_address*/, where *ip_address* is the IP address of the connector management console that you saved earlier.

> **Tip**
> If your browser can't verify the certificate for the site, it notifies you that the site is untrusted. You can verify the certificate (see Validating an Untrusted SSL Certificate (p. 48)) or replace it with one of your own certificates (see Installing a Trusted SSL Certificate (p. 48)).

2. In the **Log in to Connector** dialog box, enter the IP address or hostname of the vCenter Server and the credentials for a vCenter administrator, and then click **Log in**. The vCenter hostname can't be longer than 32 characters. Therefore, specify a shorter hostname or the IP address.

When prompted, create a password. You'll use this password the next time that you log in to the connector management console.

> **Note**
> If you enter an incorrect password 20 times, you are locked out and must reset your password. For more information, see Resetting the Connector Password (p. 43).

3. If this is the first time that you've logged in to the connector, the registration wizard starts automatically. Otherwise, click **Register the Connector**.

4. If you downloaded the configuration file, do the following:

   1. Click **Upload the configuration file**, select the configuration file, and then click **Next**.

   2. On the **vCenter Service Account Credentials** page, enter the credentials of the vCenter service account that you created in Creating the Required Accounts and Users (p. 6), and then click **Next**. For domain users, use the form *domain\username* or *username@domain*.

3. On the **AWS Credentials** page, enter the credentials of the AWS service account that you selected in Setting Up the Trust Relationship (p. 7). (You can use the same IAM user for VM Import, or use a different IAM user that also has the AWSConnector policy attached.) Click **Next**.

   Note
   If you receive an error that the AWSConnector policy for your IAM user is out of date, you must update the policy. For more information, see Updating the AWSConnector Policy (p. 45).

4. On the **Register Plugin** page, click **I agree to install the vCenter SSL certificates on this connector**. You will receive automatic upgrades for the connector unless you clear this option. Click **Register** to install the vCenter Server certificate. The authentication provider in the connector responds to vCenter Server only if it presents this certificate.

Otherwise, complete the setup as follows:

1. Click **Enter the configuration manually**, select the same configuration type that you selected earlier, and then click **Next**.

2. Enter the AMP connector key that you saved earlier, and then click **Next**.

3. On the **vCenter Admin Credentials** page, enter the IP address or hostname of the vCenter server and the name and password of a vCenter admin. The vCenter hostname can't be longer than 32 characters. Therefore, specify a shorter hostname or the IP address. Click **Next**.

   Note that this page doesn't appear the first time you configure the connector.

4. On the **vCenter Service Account Credentials** page, enter the credentials of the vCenter service account that you created in Creating the Required Accounts and Users (p. 6), and then click **Next**. For domain users, use the form *domain\username* or *username@domain*.

5. On the **AWS Credentials** page, enter the ARN of the AMP trust role and credentials of the AWS service account that you selected in Setting Up the Trust Relationship (p. 7). (You can use the same IAM user for VM Import, or use a different IAM user that also has the AWSConnector policy attached.) Click **Next**.

   Note
   If you receive an error that the AWSConnector policy for your IAM user is out of date, you must update the policy. For more information, see Updating the AWSConnector Policy (p. 45).

6. On the **Register Plugin** page, click **Register** to install the vCenter Server certificate. The authentication provider in the connector responds to vCenter Server only if it presents this certificate.

5. Exit the vSphere client and reopen it. Click **Home** and then click **AWS Management Portal**.

You've complete the setup process and are ready to start using the management portal. However, you might want to complete the following steps before you begin: Configure Time Synchronization (p. 4) and Configure Network Settings (p. 4).

Option 2: SAML-Based Authentication

You can set up the management portal to authenticate users using your identity provider (IdP).

Your users don't have direct access to AWS resources. Instead, the vSphere client gets the user's information from your identity store and uses a SAML assertion to grant the user access to AWS Management Portal for vCenter. The following diagram illustrates this process.
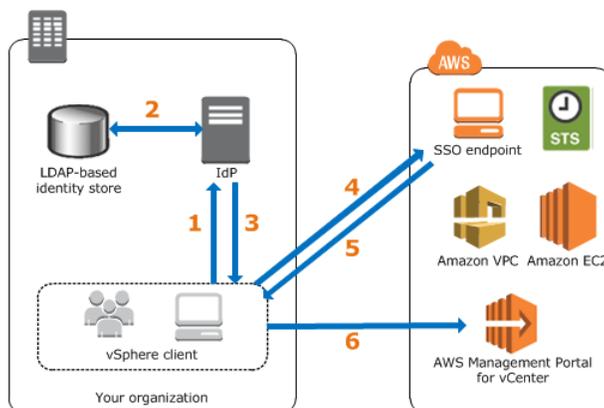
SAML-based authentication

1. The user signs in to vCenter, clicks **Home**, and then clicks **AWS Management Portal**. The vSphere client sends an authentication request to the IdP.
2. The IdP authenticates the user.
3. The IdP generates a SAML authentication response that includes assertions that identify the user and provide information about the user.
4. The vSphere client posts the SAML assertion to an AWS single sign-on (SSO) endpoint. The endpoint requests temporary security credentials from AWS Security Token Service (AWS STS) and creates a console sign-in URL.
5. AWS sends the console a sign-in URL to the vSphere client with a redirect.
6. The management portal grants users access to AWS resources based on the permissions assigned to them by an administrator.

Prerequisites

Before you get started setting up the management portal, set up and configure an IdP for use with AWS SAML federation. Your IdP must support SAML 2.0, and you must enable the `RelayState` parameter.

If you are using Windows Active Directory (AD) for your directory service, you can use Active Directory Federation Services (ADFS) as your IdP. For more information, see Setting Up ADFS for AWS Management Portal for vCenter (p. 17). For information about other identity providers, see Integrating SAML Solution Providers with AWS in *IAM User Guide*.

Tasks

To set up the management portal, complete the following tasks:

Creating the Required Accounts and Users

First, create the accounts and users that are required by the management portal.

To create the required accounts and users

1. If your organization doesn't have an AWS account already, use the following steps to create one:

a. Open https://portal.aws.amazon.com/billing/signup.

b. Follow the online instructions.

    Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

You can complete the setup process using the credentials of either your AWS account or an IAM user. For more information about AWS Identity and Access Management (IAM), see *IAM User Guide*. To allow an IAM user to set up the management portal, you must grant that user permission to use the actions specified in the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:*",
                "amp:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::export-to-s3-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```

2. Create the *AWS service account*, which is an IAM user that the connector uses to migrate VMs from vCenter to AWS.

    a. Open the IAM console at https://console.aws.amazon.com/iam/.

    b. In the navigation pane, click **Users**.

    c. Click **Add user**.

    d. On the **Add user** page, type a user name, select **Programmatic access**, and then click **Next: Permissions**.

    e. Select **Attach existing policies directly**.

    f. In the search field, type **AWSConnector**. Select the check box next for the **AWSConnector** policy and then click **Next: Review**.

    g. Click **Create user**.

    h. Save the credentials for this account in a safe location and then click **Close**.

> **Important**
> You'll need these credentials to complete the connector setup process.

3. Create the *vCenter service account*, which is a local or domain user that the connector uses to communicate with vCenter. Specify a unique, random password for the account. Do not manually assign vCenter privileges to this user at this point; we assign the vApp Export privilege to this user during the connector setup process. Note that you can restrict this privilege to specific parts of your vCenter inventory after you complete the connector setup process.

   > **Important**
   > Save the credentials for this account in a safe location. You'll need them to complete the connector setup process.

   You can create this user using your IdP, vCenter, or Windows; whichever is easiest for you. For more information about creating local or domain users, see the following documentation, or contact an administrator for your vCenter or your IdP:

   - Active Directory: Create a New User Account

   - Windows: Create a local user account

   - vCenter 5.5: Add vCenter Single Sign-On Users (the default domain is `vsphere.local`)

   - vCenter 5.1: Add a vCenter Single Sign On User (the default domain is `System-Domain`)

Setting Up the Trust Relationship

Complete the following procedure to set up a trust relationship between the management portal and your IdP.

To set up the trust relationship

1. Open the AWS Management Portal for vCenter setup console.

   > **Tip**
   > If you've already completed the setup process but would like to change authentication providers, go to the summary page, expand **Reset Trust Relationship**, click **I acknowledge that I want to reset my trust relationships configuration**, and then click **Reset Trust Relationship**.

2. Click **Get started now**.

3. On the **AWS Management Portal for vCenter Configuration** page, select **SAML-based authentication provider**.

4. On the **Configure the Trust Relationship** page, do one of the following:

   - **Option 1: Set up trust**

     1. In **SAML provider**, select **CREATE NEW** to create a SAML provider. Enter a name for the provider, select the SAML metadata document for your IdP, and then click **Save**.

        If your IdP is ADFS, you can download the SAML metadata document using the following URL, where *my-adfs-server* is the host name of your ADFS server:

        ```
        https://my-adfs-server/FederationMetadata/2007-06/FederationMetadata.xml
        ```

     2. In **Identity Provider URN**, enter the unique identifier for your IdP. This is the value of the `entityID` attribute in the SAML metadata document for your IdP.

     3. In **SAML role**, select **CREATE NEW**. This role has no AWS privileges. The management portal trusts users who can assume this role using an assertion from your IdP.

4. In **AMP service role**, select **CREATE NEW**. The management portal assumes this role to manage your AWS resources.

5. In **Import service role**, select **CREATE NEW**. The VM Import/Export service assumes this role to manage your conversion tasks when you migrate a VM using connector.

6. Click **I agree that AWS Management Portal for vCenter may create the above roles on my behalf**.

7. Click **Save and Continue**.

- **Option 2: Change authentication providers**

  If you previously selected **AWS Connector** as the authentication provider, click **Reset Trust Relationship**. After the reset, you can start the setup process again, select **SAML-based authentication provider**, and then set up trust.

5. On the **Configure Single Sign-On URL** page, enter the single sign-on (SSO) URL, and then click **Save and Continue**.

   This URL must use the following parameters: relying party identifier (`urn:amazon:webservices`) and SAML `RelayState` (`https://amp.aws.amazon.com/auth`).

   If your IdP is ADFS, the SSO URL is the IdP URL followed by:

   ```
   ?RelayState=RPID%3Durn%253Aamazon%253Awebservices%26RelayState%3Dhttps%253A%252F
   %252Famp.aws.amazon.com%252Fauth
   ```

   For example, suppose that the IdP URL is: `https://adfs.mydomain.com/adfs/ls/IdpInitiatedSignOn.aspx`. The corresponding SSO URL is:

   ```
   https://adfs.mydomain.com/adfs/ls/IdpInitiatedSignOn.aspx?RelayState=RPID%3Durn
   %253Aamazon%253Awebservices%26RelayState%3Dhttps%253A%252F%252Famp.aws.amazon.com
   %252Fauth
   ```

   You can create the SSO URL manually or use a generator tool.

6. On the **Add Administrators** page, add one to five users from your organization as administrators of the management portal, and then click **Save and Continue**. Note that you can specify both local and domain users.

   > **Important**
   > Domain and user names are case-sensitive.

   Use the form *domain\user*, where *domain* is optional for local users. For domain users, *domain\user* must not exceed 32 characters. For local users, *user* must not exceed 32 characters. The *domain* and *user* names must each begin with a letter and contain only the following characters: a-z, A-Z, 0-9, periods (.), underscores (_), and dashes (-).

   Note that you must add at least one administrator now, but you can add additional users as administrators later on. For more information, see Managing Administrators (p. 23).

7. On the **Create an AMP Connector Key** page, enter the name for the AMP connector key, and then click **Create**.

8. On the **Review Your Configuration** page, click **Download Configuration**, which downloads a file that contains your trust relationship configuration. Save this file to a safe location. You'll need it to complete the connector deployment process. Click **Finish**.

   Note that you can create a new AMP trust role or AMP connector key if you believe they were compromised.

9. Within your IdP, configure AWS as a trusted relying party. If your IdP is ADFS, see Configuring SSO to ADFS and AWS Management Portal for vCenter (p. 19) for more information.

10. Test your SSO URL using your browser. At this point, you should see a page that says the following:

```
AWS Management Portal for vCenter
Your AWS Management Portal setup is incomplete
```

If you see the AWS Management Console instead, then your IdP is not configured to support the `RelayState` parameter. For more information, see Enabling RelayState (p. 18).

Deploying the Connector Virtual Appliance

The management portal requires that you deploy and configure the connector, which manages the administrators and permissions.

The connector is packaged as a virtual appliance. To deploy the connector, complete the following procedure.

To deploy the Connector virtual appliance

1. Sign in to vCenter as a VMware administrator.

2. From the **File** menu, click **Deploy OVF Template**. Enter the following URL into the **Deploy from a file or URL** field and then click **Next**:

```
https://s3.amazonaws.com/aws-connector/AWS-Connector.ova
```

(Optional) To verify the download, use the following MD5 and SHA256 checksums:

```
https://s3.amazonaws.com/aws-connector/AWS-Connector.ova.md5sum
https://s3.amazonaws.com/aws-connector/AWS-Connector.ova.sha256sum
```

3. Complete the wizard. On the **Disk Format** page, select one of the thick provision disk types. We recommend that you select **Thick Provision Eager Zeroed**, as it has the best performance and reliability; however, it requires several hours to zero the disk. Do not select **Thin Provision**; this option makes deployment faster but significantly reduces disk performance. For more information, see Types of supported virtual disks in the VMware documentation.

4. Locate the newly deployed template in the vSphere client inventory tree, right-click it, and select **Power > Power On**. Right-click the template again and select **Open Console**. The console displays the IP address of the connector management console. Save the IP address in a secure location; you'll need it to complete the connector setup process.

> **Note**
> If you don't have a DHCP server, you must configure a static IP address. For more information, see (Optional) Configuring Network Settings (p. 4).

Configuring the Connector

To complete the setup process, open a web browser and complete the following procedure.

> **Important**
> The directions in this procedure are written for version 2.1.0 and later of the connector. If the version information in the upper-right corner of the screen is **Version: 2.0.0**, download the PDF file Configuring the Connector for directions written for version 2.0.0 of the connector.

To configure the connector using the connector management console

1. From your web browser, go to https://*ip_address*/, where *ip_address* is the IP address of the connector management console that you saved earlier.

    > **Tip**
    > If your browser can't verify the certificate for the site, it notifies you that the site is untrusted. You can verify the certificate (see Validating an Untrusted SSL Certificate (p. 48)) or replace it with one of your own certificates (see Installing a Trusted SSL Certificate (p. 48)).

2. In the **Log in to Connector** dialog box, enter the IP address or hostname of the vCenter Server and the credentials for a vCenter administrator, and then click **Log in**. The vCenter hostname can't be longer than 32 characters. Therefore, specify a shorter hostname or the IP address.

    When prompted, create a password. You'll use this password the next time that you log in to the connector management console.

    > **Note**
    > If you enter an incorrect password 20 times, you are locked out and must reset your password. For more information, see Resetting the Connector Password (p. 43).

3. If this is the first time that you've logged in to the connector, the registration wizard starts automatically. Otherwise, click **Register the Connector**.

4. On the **Upload Key Pair** page, copy the key that you created when setting up the trust relationship, and then click **Next**.

5. On the **vCenter Admin Credentials** page, enter the credentials of a vCenter account that has permissions to register a new vCenter extension, and then click **Next**. Note that we discard these credentials after you complete the connector setup process.

6. On the **vCenter Service Account Credentials** page, enter the credentials of the vCenter service account that you created in Creating the Required Accounts and Users (p. 11), and then click **Next**. For domain users, use the form *domain\username* or *username@domain*.

    Note that we store these credentials in encrypted form, and you do not need to store them after you complete the setup process.

7. On the **AWS Credentials** page, enter the credentials of the AWS service account that you created in Creating the Required Accounts and Users (p. 11), and then click **Next**. Note that we store these credentials in encrypted form.

    > **Note**
    > If you receive an error that the AWSConnector policy for your IAM user is out of date, you must update the policy. For more information, see Updating the AWSConnector Policy (p. 45).

8. On the **Register Plugin** page, click **Register**.

9. Exit the vSphere client and reopen it. Click **Home** and then click **AWS Management Portal**.

    If you are prompted to select an IAM role, select the role with `AWS-Management-Portal-for-vCenter` in its name.

    > **Important**
    > If you see the AWS console instead of the management portal, it is probably because the `RelayState` parameter is not enabled. For more information, see Enabling RelayState (p. 18).

You've completed the setup process and are ready to start using the management portal. However, you might want to complete the following steps before you begin: Configure Time Synchronization (p. 4) and Configure Network Settings (p. 4).

Setting Up ADFS for AWS Management Portal for vCenter

If you are using Windows Active Directory (AD) as your directory service, you can use Active Directory Federation Services (ADFS) as your identity provider (IdP) and enable federated single sign-on (SSO) to your AWS environment.

To enable integration between your organization and AWS, complete the following tasks.

Tasks

Requirements

Prepare the following requirements:

- Create a domain account in Active Directory. For example, we use the name `adfssvc` in these procedures. Keep the password in a safe place. You'll use this account as the ADFS service account later in this procedure.
- Verify that the server to run ADFS is joined to the domain. You can also update the computer name.
- (Optional) If you don't have a certificate, you can create a self-signed certificate using Internet Information Services (IIS). It's convenient to use a self-signed certificate in a development environment. However, you'll need a certificate from a trusted certificate authority for a production environment.

  To create a self-signed certificate

  1. Open Internet Information Services (IIS) Manager.
  2. In the **Connections** pane, select a server node.
  3. From the **Home** page for the server node, open **Server Certificates**.
  4. From the **Actions** pane, click **Create Self-Signed Certificate**.
  5. In the **Create Self-Signed Certificate** dialog box, specify a name for the certificate, and then click **OK**.

Installing ADFS 3.0

If you have not done so already, install ADFS on your server and configure it as a federation server.

To install ADFS 3.0 on Windows Server 2012

1. Open Server Manager.
2. From the dashboard, click **Add roles and features**.
3. On the **Select installation type** page, select **Role-based or feature-based installation** and then click **Next**.
4. On the **Select destination server** page, select **Select a server from the server pool**, select your server from the list, and then click **Next**.
5. On the **Select server roles** page, select **Active Directory Federation Services** and then click **Next**.
6. On the **Confirm installation selections** page, click **Install**.

To configure ADFS 3.0

1. Open Server Manager and click the warning icon to complete post-deployment configuration.
2. On the **Welcome** page, select **Create the first federation server in a federation server farm**, and then click **Next**.
3. On the **Connect to Active Directory Domain Services** page, specify a domain administrator account, and then click **Next**.
4. On the **Specify Service Properties** page, select the SSL certificate described in the Requirements section. Click **Import**. Provide the requested information, and then click **Next**.
5. On the **Specify Service Account** page, click **Use an existing domain user account or group Managed Service Account**. Specify the domain account described in the Requirements section (for example, `adfssvc`).
6. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database** and then click **Next**.
7. Review the information on the **Review Options** page, and then click **Next**.
8. On the **Pre-requisite Checks** page, monitor the status of the checks. Address any issues that are reported. When all checks pass successfully, click **Configure**.

   If you see an error message that begins with "An error occurred during an attempt to set the SPN for the specified service account," you can fix the issue by opening a Command Prompt window as an administrator and then running the following command:

   ```
   setspn –a host/localhost service-account
   ```

   Note that `service-account` is the name of the service account described in the Requirements section (for example, `adfssvc`). Upon success, the output for this command ends with "Updated object."

Enabling RelayState

Before you continue, verify that your ADFS supports the `RelayState` parameter, and then enable it. This parameter was introduced in Update Rollup 2 for ADFS 2.0. This parameter is supported in ADFS 3.0, but it is not enabled by default.

To enable RelayState

1. [ADFS 2.0] In Control Panel, go to Installed Updates and look for update KB2681584 (Update Rollup 2) or KB2790338 (Update Rollup 3).
2. In a text editor, such as Notepad, open the following file:

   - [ADFS 2.0] `C:\inetpub\adfs\ls\web.config`
   - [ADFS 3.0] `%systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config`

3. In the `microsoft.identityServer.web` section, add `useRelyStateForIdpInitiatedSignOn` as follows, and save the change:

   ```
   <microsoft.identityServer.web>
       ...
       <useRelayStateForIdpInitiatedSignOn enabled="true" />
   </microsoft.identityServer.web>
   ```

4. [ADFS 2.0] Restart IIS using the following command:

   ```
   C:\> IISReset
   ```

```
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
```

5. Restart ADFS as follows:

   a. On the **Start** menu, point to **Administrative Tools**, and then click **Services**.

   b. Right-click the ADFS service, and then click **Restart**.

# Configuring SSO to ADFS and AWS Management Portal for vCenter

You can configure single sign-on (SSO) between ADFS and the management portal. When a user requests access to AWS through the management portal, ADFS authenticates the user.

> **Note**
> If you have already set up a trust relationship with AWS, edit the `NameId` claim to match the configuration in step 11 (the incoming claim type is `Windows account name`, the outgoing claim type is `Name Id`, and `Persistent Identifier` is the outgoing name ID format). Then, continue with step 15.

To configure trust between AWS and ADFS

1. [ADFS 2.0] From the **Start** menu, open **AD FS 2.0 Management**.

   [ADFS 3.0] From Server Manager, click **Tools**, and then select **AD FS Management**.

2. [ADFS 2.0] In the **Actions** pane, click **Add Relying Party Trust**.

   [ADFS 3.0] Under **AD FS\Trust Relationships**, right-click **Relying Party Trusts** and then click **Add Relying Party Trust**.

3. On the **Welcome** page, click **Start**.

4. On the **Select Data Source** page, select **Import data about the relying party published online or on a local network**. Enter "https://signin.aws.amazon.com/static/saml-metadata.xml" as the federation metadata address, and then click **Next**.
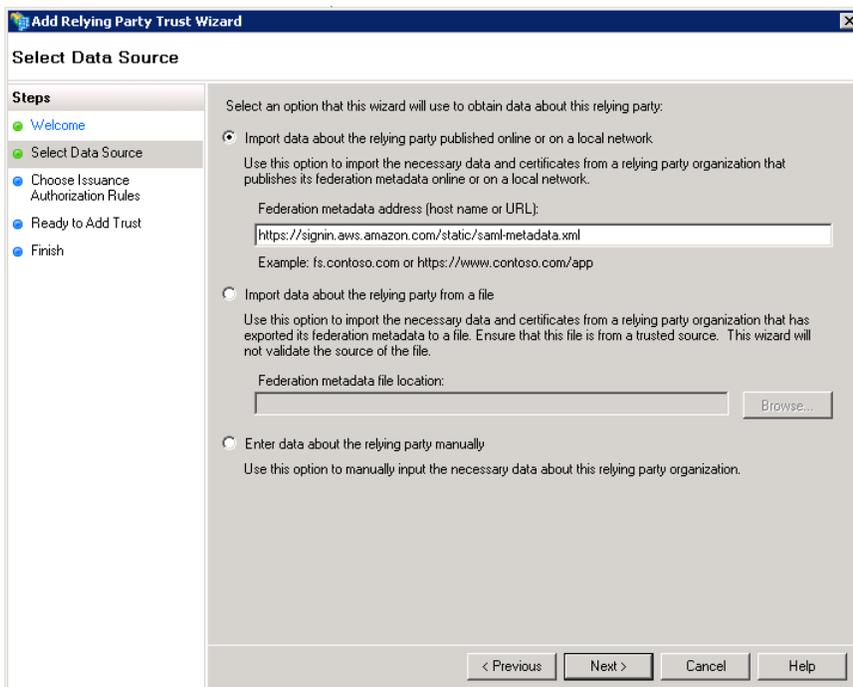
5. On the **Specify Display Name** page, enter "AWS Management Portal for vCenter" as the display name, and then click **Next**.
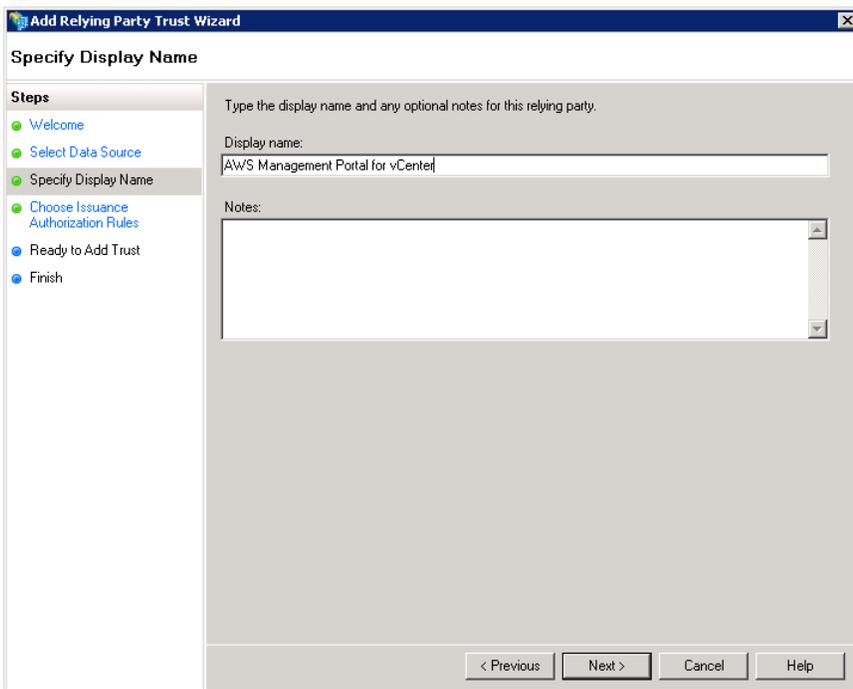

6. On the **Choose Issuance Authorization Rules** page, select **Permit all users to access this relying party**, and then click **Next**.

7. On the **Ready to Add Trust** page, review your settings, and then click **Next**.

8. On the **Finish** page, select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes**, and then click **Close**.

9. In the **Edit Claim Rules for AWS Management Portal for vCenter** dialog box, on the **Issuance Transform Rules** tab, click **Add Rule**.

10. On the **Select Rule Template** page, select the **Send Claims Using a Custom Role** claim rule template from the list, and then click **Next**.

11. To configure the claim rule, enter `NameId` in **Claim rule name**, enter the following rule in **Custom claim rule**, and then click **Finish**.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/
windowsaccountname"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:persistent");
```

Use the Windows user name (*domain\user*) as the `NameId` claim. Ensure that these names are less than 32 characters long and are persistent identifiers.
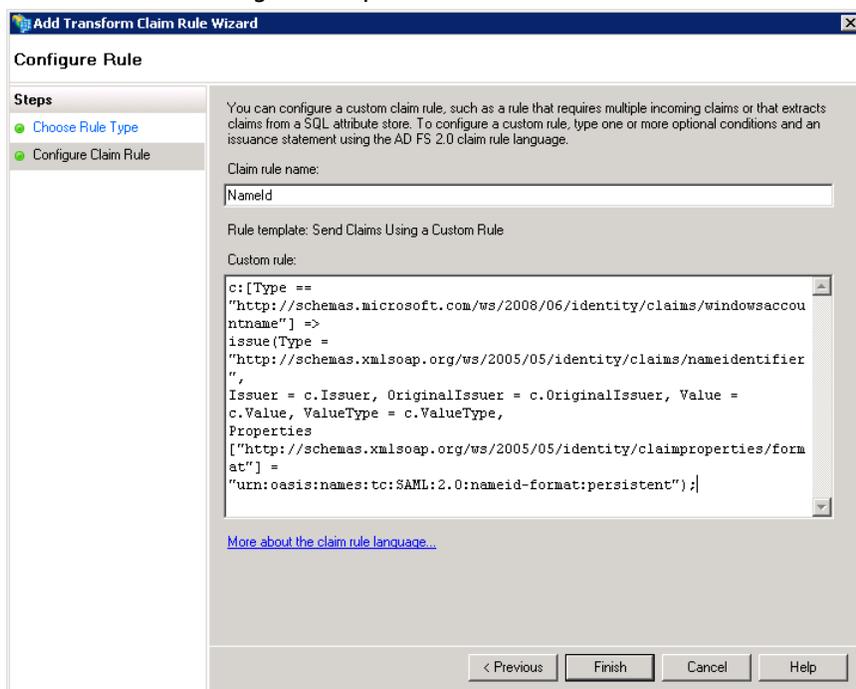
12. Click **Add Rule**.

13. Select **Send Claims Using a Custom Role**, and then click **Next**.

14. To configure the claim rule, enter `RoleSessionName` in **Claim rule name**, enter the following rule in **Custom claim rule**, and then click **Finish**.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/
windowsaccountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types = ("https://aws.amazon.com/SAML/Attributes/
RoleSessionName"),
query = ";mail;{0}", param = c.Value);
```

Use the display name for the user with the SAML assertion. These names must be less than 32 characters long and contain only the following set of characters: [a-zA-Z_0-9+=,.@-].

The user must have an email address set up in Active Directory.

15. Click **Add Rule**.

16. Select **Send Claims Using a Custom Role**, and then click **Next**.

17. To configure the claim rule, enter `AmpRole` in **Claim rule name**, enter the following rule in **Custom claim rule**, and then click **Finish**.

```
=> issue(Type="https://aws.amazon.com/SAML/Attributes/Role", Value =
"arn:aws:iam::account_id:saml-
provider/provider_name,arn:aws:iam::account_id:role/saml_role");
```

This rule requires the ARNs of the SAML provider (arn:aws:iam::*account_id*:saml-provider/*provider_name*) and the SAML role (arn:aws:iam::*account_id*:role/*saml_role*). You can look up these ARNs using the AWS Management Portal for vCenter setup console.

18. Start and stop the ADFS service and test this configuration. AWS trusts the users authorized by the IdP to assume the SAML role. Therefore, be sure that your IdP authenticates and authorizes a user in your network before granting an assertion.

Administering AWS Resources Using AWS Management Portal for vCenter

Administrators for AWS Management Portal for vCenter are responsible for managing an AWS network, known as a virtual private cloud (VPC), creating environments, and granting users permission to access environments.
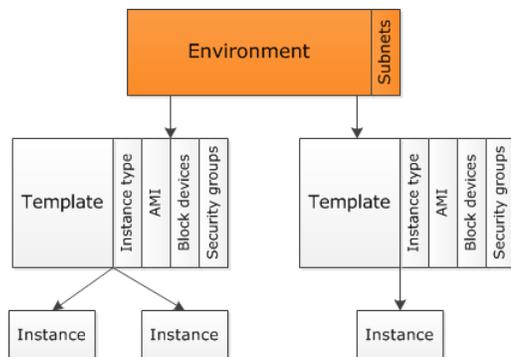
Contents

Managing Administrators

We recommend that you select several users to administer the management portal. To add an administrator for the management portal, you must be an administrator for both vCenter and the management portal.

To add an administrator

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. From the top pane, click **Admin Users**.
3. Click **Add**.

    Tip
    If you are using the connector to authenticate users and it is in maintenance mode, you'll receive the error "Unable to contact User Provider. Please contact your Administrator." We recommend that you wait a few minutes and then try again.
4. In the **Select Users** dialog box, select the domain and one or more users, and then click **OK**.

    Note that domains and users are disabled if their names don't meet certain requirements. If a user is a domain user, *domain\user* must not exceed 32 characters. If a user is a local user, *user* must not exceed 32 characters. The *domain* and *user* values must each begin with a letter and contain only the following characters: a-z, A-Z, 0-9, periods (.), underscores (_), and dashes (-).

5. When you are finished adding administrators, click **Save**.

To remove an administrator for the management portal, you must be an administrator for the management portal.

To remove an administrator

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. Click **Admin Users**.
3. Select the user from the list.
4. Click **Remove**, and then click **Save**.

Managing VPCs and Subnets

By default, you can create up to five VPCs per region. You can create one or more subnets per VPC and one or more security groups per VPC. To configure route tables, network ACLs, and other advanced VPC features, you must use the AWS Management Console or the AWS CLI. For more information about VPCs, see the Amazon VPC User Guide.

Note that each region might also have a default VPC, depending on when you created your AWS account.

To create a VPC and subnets

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. From the top pane, click **VPC**.
3. Select a region for the VPC. On the **Getting Started** tab, click **Create a virtual private cloud**.
4. Enter a name for the VPC in **VPC Name**.
5. Select the configuration that meets your needs, **VPC with a single public subnet** or **VPC with public and private subnets**, and then click **Next**.

    Note that you can add additional subnets after you create the VPC. Also, the Amazon VPC console supports additional configurations for your VPC.
6. Enter an IP address range for the VPC, in CIDR notation (for example, `10.0.0.0/16`).
7. For each subnet, enter an IP address range, in CIDR notation (for example, `10.0.0.0/24`), and select an Availability Zone. Note that if you create multiple subnets in a VPC, the IP address ranges for the subnets must not overlap. When you are finished, click **Next**.
8. (Optional) Specify one or more tags for your VPC. For each tag, click **Add**, enter the tag key, and enter the tag value.
9. When you are finished adding tags, click **Finish**.
10. (Optional) To add another subnet to your VPC, select the VPC, and then click **Create a subnet** on the **Getting Started** tab. Enter a name, select an Availability Zone, and enter an IP address range for the subnet, in CIDR notation. By default, the subnet is a public subnet. To create a private subnet, click **Make this a private subnet**. You can also specify one or more tags for the subnet. When you are finished, click **Finish**.

You can delete a nondefault VPC only if there are no running instances in its subnets. You can't delete a default VPC using the management portal.

To delete a VPC

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. Click **VPC**.

3. Expand the region for the VPC, and then select the VPC.
4. On the **Getting Started** tab, click **Delete the virtual private cloud**.
5. In the **Delete VPC** dialog box, click **Yes**.

Managing Security Groups

A security group acts as a firewall that controls the traffic for one of more EC2 instances. You'll create a security group and add rules that allow users to connect to EC2 instances in the VPC associated with the security group. Users select one or more security groups when they create a template.

To create a security group

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. From the top pane, click **VPC**.
3. Expand the region for the VPC, and then select the VPC.
4. On the **Getting Started** tab, click **Create a security group**.
5. Enter a name and a description for the security group, and then click **Next**.
6. To connect to an EC2 Linux instance, you must add a rule that allows inbound traffic using SSH. (Note that you can skip this step and add the rule later by selecting the security group and clicking **Add a rule** on the **Getting Started** tab.)

   a. Click **Add**.
   b. From the **Type** list, select **SSH**.
   c. From the **Source** list, select **Custom IP**.
   d. Enter the IP address range in **IP**, in CIDR notation. For example, if your IP address is `203.0.113.25`, specify `203.0.113.25/32` to list this single IP address in CIDR notation. If your company allocates addresses from a range, specify the entire range, such as `203.0.113.0/24`.
   e. Verify that **Inbound** is selected.
   f. Click **Add**.
7. To connect to an EC2 Windows instance, you must add a rule that allows inbound traffic using RDP. (Note that you can skip this step and add the rule later by selecting the security group and clicking **Add a rule** on the **Getting Started** tab.)

   a. Click **Add**.
   b. From the **Type** list, select **RDP**.
   c. From the **Source** list, select **Custom IP**.
   d. Enter the IP address range in **IP**, in CIDR notation. For example, if your IP address is `203.0.113.25`, specify `203.0.113.25/32` to list this single IP address in CIDR notation. If your company allocates addresses from a range, specify the entire range, such as `203.0.113.0/24`.
   e. Verify that **Inbound** is selected.
   f. Click **Add**.
8. When you are finished adding rules, click **Next**.
9. (Optional) Specify one or more tags for your security group. For each tag, click **Add**, enter the tag key, and enter the tag value. When you are finished entering tags, click **Next**.
10. Review the properties for your security group. To make changes, click **Back**. When you are ready to create the security group, click **Finish**.

You can delete a security group only if it's not currently associated with an instance.

To delete a security group

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. Click **VPC**.
3. Expand the region and the VPC for the security group, and then select the security group.
4. On the **Getting Started** tab, click **Delete the security group**.
5. In the **Delete Security Group** dialog box, click **Yes**.

To change the security groups for a running instance, you must use the Amazon EC2 console or the AWS CLI. For more information, see Security Groups for Your VPC in the *Amazon VPC User Guide*.

Managing Environments

Administrators use *environments* to organize and manage AWS resources. They grant permissions to users at the environment level.

As an administrator, you can create environments, and you have access to default environments. The *default environment* for a region enables you to manage EC2 instances that were created for your AWS account in that region using tools such as the AWS Management Console, the AWS CLI, or an AWS SDK, instead of using the management portal.

To create an environment

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. From the top pane, click **Dashboard**.
3. Select a region for the environment. On the **Getting Started** page, click **Create an environment**.
4. Enter a name for the environment in **Name**.
5. Select a VPC from **VPC**. Note that this list includes all VPCs for the region, including VPCs created using the Amazon VPC console and the default VPC (if it exists). If this list is empty, you must create a VPC in this region.
6. Select one or more subnets from **Subnets**. Note that this list includes all subnets for the selected VPC, including any default subnets. If this list is empty, you must add a subnet to the VPC or select a different VPC.
7. Click **Finish**.

After you create an environment, you create one or more templates and use these templates to launch EC2 instances into your environment. For more information, see Managing EC2 Instances Using AWS Management Portal for vCenter (p. 29). When you launch an instance, we add a tag with the name `aws-management-portal/environment-id` and the value set to the ID of the environment. You can use this tag to track resources using detailed billing reports or EC2 usage reports. Users can't modify this tag using the management portal. However, users may have access to modify or delete this tag using the Amazon EC2 console, CLI, or API. If someone modifies or deletes this tag, it can affect users' permissions to access the instance. Therefore, we recommend that you limit the users who can create, modify, or delete tags.

You can delete an environment only after you've deleted its templates.

To delete an environment

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. Click **Dashboard**.
3. Expand the region for the environment, and then select the environment.

4. Right-click the environment and select **Delete**.

5. In the **Delete Environment** dialog box, click **Yes**.

Administrators can describe, start, stop, reboot, and terminate EC2 instances in the default environment for a region using the management portal.

To manage instances in the default environment

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.

2. Click **Dashboard** and expand the region.

3. To list your instances, do one of the following:

   - Expand **Default Environment**.
   - Click **Default Environment** and then click the **Instances** tab.

4. To start, stop, reboot, or terminate an instance, expand **Default Environment** and select the instance. From the **Getting Started** tab, click the desired task under **Basic Tasks**.

Managing User Permissions

Administrators can manage users' permissions to access an environment. To grant permissions, you must be an administrator for both vCenter and the management portal. To edit or delete permissions, you must be an administrator for the management portal.

The specific permissions granted to a user depend on the role that you assign to the user. The management portal defines the following roles:

`No-Access`

   No permissions.

`Read-Only`

   Permissions to view the environment, including its templates and instances.

`General`

   Includes permissions from `Read-Only`, plus permissions to run, rename, reboot, stop, start, terminate, and import instances.

`Owner`

   Includes permissions from `General`, plus permissions to create, delete, and rename templates, to import and delete key pairs, and to create images.

To grant permissions to a user

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.

2. From the top pane, click **Dashboard**.

3. Expand the region for the environment, right-click the environment, and then click **Add Permission**.

4. Click **Add**. In the **Select Users** dialog box, select the domain and one or more users, and then click **OK**.

   Note that domains and users are disabled if their names don't meet certain requirements. If a user is a domain user, *domain\user* must not exceed 32 characters. If a user is a local user, *user* must not exceed 32 characters. The *domain* and *user* values must each begin with a letter and contain only

the following characters: a-z, A-Z, 0-9, periods (.), underscores (_), and dashes (-). Capitalization of domain and user should match that of the vCenter user.

5. Select one or more users from **Users**, and then select a role from **Assigned Role**.
6. Click **Save**. The changes are displayed in the **Permissions** tab.

To change the permissions granted to a user

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. Click **Dashboard**.
3. Expand the region for the environment, and then select the environment.
4. From the **Permissions** tab, right-click the user and select **Properties**.
5. Select a different role and click **Save**. The updates are displayed in the **Permissions** tab.

**To revoke the permissions granted to a user**

1. Sign in to vCenter as an administrator, click **Home**, and then click **AWS Management Portal**.
2. Click **Dashboard**.
3. Expand the region for the environment, and then select the environment.
4. From the **Permissions** tab, right-click the user and select **Delete**.
5. When prompted for confirmation, click **OK**. The updates are displayed in the **Permissions** tab.

Managing EC2 Instances Using AWS Management Portal for vCenter

You can launch an EC2 instance using the management portal. First, create a template from an environment set up by an administrator, then deploy the instance from the template. You can view, stop, start, and terminate the instance. Note that your ability to complete these tasks depends on the permissions granted to you by your administrator.
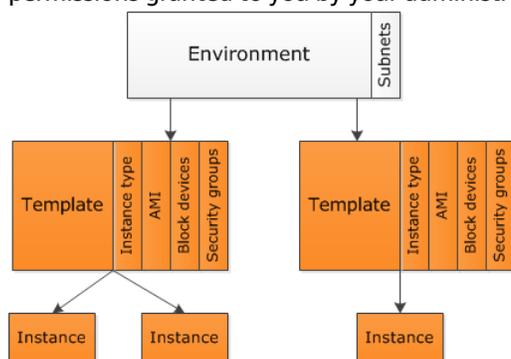
Note
We recommend using AWS Server Migration Service (SMS) to migrate VMs from a vCenter environment to AWS. SMS automates the migration process by replicating on-premises VMs incrementally and converting them to Amazon machine images (AMIs). You can continue using your on-premises VMs while migration is in progress. For more information about AWS SMS, see AWS Server Migration Service.

Contents

Viewing Regions

The first time that you log in to the management portal, you are asked to select the regions to display in the dashboard. You can update the regions displayed in the dashboard at any time. For example, if you don't have AWS resources in some regions, you can exclude them from the dashboard. If later on you need to create resources in a region that's not displayed, you can include it in the dashboard.

To select the regions to display

1. From the menu in the upper-right corner, select **Region Preferences**.
2. Choose the regions to display.
3. Click **Save**.

Viewing an Environment

Your AWS resources are organized and managed using environments. The permissions that you've been granted by your administrator determine whether you can view an environment, along with its templates and instances.

To view an environment

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region for the environment, and then select the environment.
3. To display information about the environment, click the **Summary** tab.
4. To list the instances deployed using the templates of this environment, click the **Instances** tab.

Managing Key Pairs

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information for your instance. Public-key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a *key pair*.

To connect to your instance, you must create a key pair, import the public key to the environment for the instance, and select it when you create the template from which you'll deploy the instance. You'll use the private key when you connect to the instance that you launch using this template.

The permissions that you've been granted by your administrator determine whether you can import a key pair.

To import a key pair

1. Create an RSA key pair using a tool like ssh-keygen. Save the public key to a local file, and the private key to a different local file with the `.pem` extension. For more information, see Amazon EC2 Key Pairs in the *Amazon EC2 User Guide*.
2. From vCenter, click **Home** and then click **AWS Management Portal**.
3. From the dashboard, expand the region for the environment, and then select the environment.
4. Click the **Key Pairs** tab.
5. Right-click in the unused space in the tab and select **Import Key Pair**.
6. In the **Import Key Pair** dialog box, click **Browse**. Select the public key file that you created in step 1 and then click **Import**.

When you no longer need to deploy instances using a key pair, or if you lose the private key, you can delete the public key that you imported. The permissions that you've been granted by your administrator determine whether you can delete a key pair.

To delete a key pair

1. From vCenter, click **Home** and then click **AWS Management Portal**.

2. From the dashboard, expand the region for the environment, and then select the environment.

3. Click the **Key Pairs** tab.

4. Right-click the key pair and select **Delete Key Pair**.

5. When prompted to confirm, click **Yes**.

Managing Templates

A template specifies the information that Amazon EC2 requires when configuring an instance. The permissions that you've been granted by your administrator determine whether you can create a template.

To create a template

1. From vCenter, click **Home** and then click **AWS Management Portal**.

2. From the dashboard, expand a region for the template, and then select the environment for the template.

3. On the **Getting Started** tab, click **Create a template**. If this task isn't listed, your administrator didn't grant you permission to create templates in this environment.

4. Enter a name for the template in **Name**.

5. By default, the Quick Start AMIs, a selection of popular AMIs, are displayed. To filter by platform, click **Windows** or **Linux**. To use a specific AMI, select **Search by AMI ID** from **AMIs from**, type the ID of the AMI, and then click **Load**.

   Note that the root device for a Linux AMI is either an Amazon EBS volume or an instance store volume. For more information about how the root device type affects the instance, see Storage for the Root Device in the *Amazon EC2 User Guide*.

6. Select an AMI and then click **Next**.

7. Select an instance type from **Instance Type**. Note that this list includes only the instance types supported by the selected region.

8. (Optional) If you'd like to connect to your instance, select **Associate Public IP Address**.

9. Select a subnet and then click **Next**.

10. (Optional) Review the storage devices specified by the AMI. To add a new storage device to the list, click **Add**. In the **Add Volume** dialog box, select a volume type, a device name, and either a volume size or a snapshot, and then click **Add**.

11. When you are finished adding volumes, click **Next**.

12. Select one or more security groups, and then click **Next**.

13. Click **Select one of your existing key pairs**, select a key pair from the list, and then click **Finish**. If the list is empty, there are no imported key pairs for this environment. For more information, see Managing Key Pairs (p. 30).

You can create a new template by starting with an existing one.

To copy and update a template

1. From vCenter, click **Home** and then click **AWS Management Portal**.

2. From the dashboard, expand the region and the environment for the template, and then select the template.

3. On the **Getting Started** tab, click **Copy to a new template**. If this task isn't listed, your administrator didn't grant you permission to create templates in this environment.

4. Click **Next** to review each page. When you have finished making changes to the new template, click **Finish**.

You can delete a template only after you terminate all instances that were launched using the template. For more information, see Terminating an EC2 Instance (p. 34). The permissions that you've been granted by your administrator determine whether you can delete a template.

To delete a template

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region and the environment for the template, and then select the template.
3. On the **Getting Started** tab, click **Delete the template**. If this task isn't listed, your administrator didn't grant you permission to delete templates in this environment.
4. In the **Delete Template** dialog box, click **Yes**.

Deploying an EC2 Instance

You deploy an EC2 instance into a subnet using a template. The permissions that you've been granted by your administrator determine whether you can deploy an EC2 instance.

To deploy an EC2 instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region and the environment for the instance, and then select the template.
3. On the **Getting Started** tab, click **Deploy an instance**. If this task isn't listed, your administrator didn't grant you permission to deploy instances in this environment.
4. Enter a name for the instance in **Name**.
5. (Optional) Specify one or more tags for your instance. For each tag, click **Add**, type the tag key, and type the tag value.
6. When you are finished adding tags, click **Next**.
7. Select a subnet for the instance to run in and then click **Next**. Note that the subnet list includes only the subnets for the selected template.
8. Review the configuration for your instance. To make changes, click **Back**. When you are ready to deploy the instance, click **Finish**.

Viewing an EC2 Instance

You can describe one or more EC2 instances. The permissions that you've been granted by your administrator determine whether you can describe EC2 instances.

To view an EC2 instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region for the instance, and then select an environment.
3. To display information about the instances deployed using the templates of this environment, click the **Instances** tab. Note that this tab also contains any instances that you migrated from a VM.
4. Select a template. To display information about the instances deployed using this template, click the **Instances** tab.
5. Expand a template that you've used to deploy instances, and then select an instance.
6. To display information about the instance, click the **Summary** tab. To display performance data for the instance, click the **Performance** tab.

Connecting to an EC2 Instance

You can log in to an EC2 instance if you have the private key (.pem file) of the key pair associated with the template that you used to launch the instance. If you need to connect to your instance, but there isn't a key pair associated with the template, you must terminate the instance, create (or ask your administrator to create) a new template (selecting a key pair in the process), and launch a new instance from the new template.

The tool that you'll use to connect to your instance depends on whether the instance is a Windows instance or a Linux instance.

To connect to an EC2 Windows instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region, the environment, and the template for the instance.
3. Select the instance.
4. On the **Summary** tab, locate the public DNS name. You'll need this information to connect to your instance.
5. On the **Summary** tab, click **Get Windows Password**. Follow the directions to get the password for the Administrator account for your instance, using the private key of the key pair for the template that you used to launch the instance. You'll need this password to connect to your instance.
6. Connect to the instance using an RDP client. Specify the public DNS name for the instance as the computer name and specify Administrator as the user name. When prompted for credentials, use the password that you got in the previous step.

   If you can't connect to the instance successfully, see Troubleshooting Windows Instances in the *Amazon EC2 User Guide for Windows Instances*.

To connect to an EC2 Linux instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region, the environment, and the template for the instance.
3. Select the instance.
4. On the **Summary** tab, locate the public DNS name. You'll need this information to connect to your instance.
5. Connect to the instance using PuTTY. For more information, see Connect to Linux Instances Using PuTTY in the *Amazon EC2 User Guide for Linux Instances*.

Stopping and Starting an EC2 Instance

You can stop and start an instance only if it has an Amazon EBS volume as its root device. If you stop and start an instance, you'll lose any data on the instance store volumes for the instance.

The permissions that you've been granted by your administrator determine whether you can stop and start an EC2 instance.

To stop and start an EC2 instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region, the environment, and the template for the instance.
3. Select the instance.

4. On the **Getting Started** tab, click **Stop the instance**. If this task isn't listed, your administrator didn't grant you permission to stop instances in this environment.

5. When you are ready for the instance to run again, select the instance and click **Start the instance**.

Rebooting an EC2 Instance

An instance reboot is equivalent to an operating system reboot. In most cases, it takes only a few minutes to reboot your instance.

The permissions that you've been granted by your administrator determine whether you can reboot an EC2 instance.

To reboot an EC2 instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region, the environment, and the template for the instance.
3. Select the instance.
4. On the **Getting Started** tab, click **Reboot the instance**. If this task isn't listed, your administrator didn't grant you permission to reboot instances in this environment.

Creating an Image from an EC2 Instance

You can create an Amazon Machine Image (AMI) from an Amazon EBS-backed instance as follows.

To create an Amazon EBS-backed image

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region, the environment, and the template for the instance.
3. Select the instance.
4. On the **Getting Started** tab, click **Create image**. If this task isn't listed, your administrator didn't grant you permission to create images in this environment.
5. In the **Create image** dialog box, do the following:

   a. Specify a name and description for the image.
   b. (Optional) To include additional volumes, click **Add New Volume**, and select the volume type and device name. For EBS volumes, you must also specify a volume size or a snapshot.
   c. Click **Create**.

Terminating an EC2 Instance

When you've decided that you no longer need an instance, you can terminate it. After you terminate an instance, you can't connect to or recover the instance. For more information about the difference between stopping and terminating an instance, see Instance Lifecycle in the *Amazon EC2 User Guide*.

The permissions that you've been granted by your administrator determine whether you can terminate an EC2 instance.

To terminate an EC2 instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.

2. From the dashboard, expand the region, the environment, and the template for the instance.

3. Select the instance.

4. On the **Getting Started** tab, click **Terminate the instance**. If this task isn't listed, your administrator didn't grant you permission to terminate instances in this environment.

Migrating Your Virtual Machine to Amazon EC2 Using AWS Connector for vCenter

You can launch an EC2 instance from a virtual machine that you migrate from VMware vCenter to Amazon EC2. You'll use the AWS Connector for vCenter to migrate your virtual machines to Amazon EC2.

The following diagram illustrates the migration process. When you request a migration, we create a conversion task. When the conversion task completes successfully, your imported instance is available.
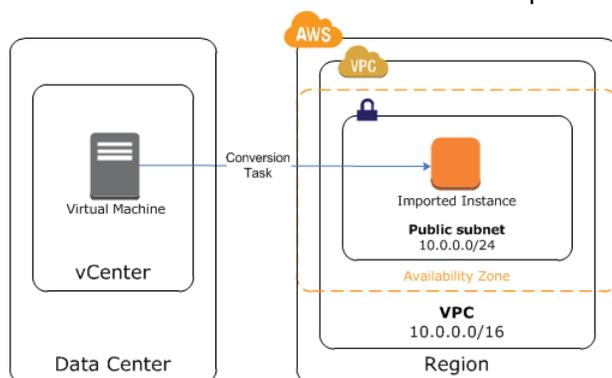
To migrate from vCenter 6.5, to specify the BYOL license type during migration, or to use incremental migration, use AWS Server Migration Service instead. For more information, see the AWS SMS User Guide.

> **Note**
> We recommend using AWS Server Migration Service (SMS) to migrate VMs from a vCenter environment to AWS. SMS automates the migration process by replicating on-premises VMs incrementally and converting them to Amazon machine images (AMIs). You can continue using your on-premises VMs while migration is in progress. For more information about AWS SMS, see AWS Server Migration Service.

Contents

Prerequisites

- An administrator must install and configure the connector. The connector is part of AWS Management Portal for vCenter. For more information, see Setting Up AWS Management Portal for vCenter (p. 3).

- An administrator must create at least one environment and grant you permission to migrate a virtual machine into one or more environments. This environment is in addition to the default environment and must be explicitly created. For more information, see Managing Environments (p. 26).
- Ensure that your VM uses one of the supported operating systems and that you select one of the supported instance types. For more information, see VM Import/Export Prerequisites in the *Amazon EC2 User Guide*.
- Attach the `VMImportExportRoleForAWSConnector` policy to the **vmimport** role that you created per VM Import Service Role in the *Amazon EC2 User Guide*.
- Ensure that your VM does not have a disk whose compressed size is greater than 215 GB.

Limitations

- Review VM Import/Export Requirements and Limitations in the *Amazon EC2 User Guide*.
- Amazon EC2 limits the number of active migrations to 5 per region. If the connector is already in the process of migrating 4 virtual machines, it queues any additional migration tasks until one of the active migration tasks completes successfully or is canceled.

VM Import Authorization

Your users don't have direct access to AWS. The following diagram describes the process by which a user can migrate a VM to Amazon EC2.
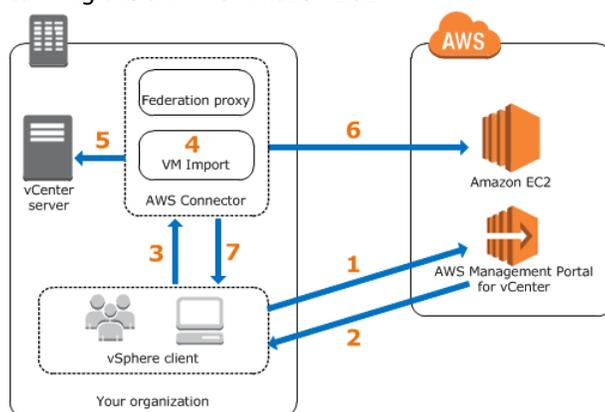
1. The vSphere client authorizes import to the environment.
2. The management portal verifies that the user has permission to migrate VMs to the environment and returns a token.
3. The vSphere client sends an import request to the connector along with the token.
4. The connector verifies the token.
5. The connector verifies that the user has permission to export the VM.
6. The connector starts the migration.
7. The connector sends a response to the vSphere client with the import task ID.

Migrating Your Virtual Machine

To migrate a VM to Amazon EC2, use vCenter with the connector. The connector can migrate up to four VMs concurrently.

Warning
You can't create a migration task while the connector is updating.

To migrate your virtual machine to Amazon EC2

1. From vCenter, click **Home** and then click **VMs and Templates**.
2. Select the VM.
3. Right-click the VM, and then click **Migrate VM to EC2**. If your administrator did not grant you permission to migrate VMs, you'll see a message to ask your administrator to grant you permission.
4. Complete the form as follows:

   a. Select the operating system running on the VM.
   b. Select the region and environment for the resulting EC2 instance. The list of environments contains only the environments to which your administrator has granted you permission.
   c. Select a subnet, instance type, and security group for the instance.
   d. (Optional) Enter a private IP address. If you don't specify a private IP address, we'll select one for you.
   e. Select a security group. The list of security groups contains only the security groups associated with the environment you've selected.
   f. Click **Begin migration to Amazon EC2**.
   g. [Prior to connector 2.4.0] If the connector displays a warning that there are already four active migration tasks and that this will affect the speed of these tasks, you can either continue or cancel the migration task.
5. After the migration begins, we display the import task ID if the migration task started immediately or the queued task ID otherwise. Note the ID if you want to monitor the migration task. Otherwise, you can close the import window and your vSphere client after the connector notifies you that the import task was created or queued, and the migration will continue.
6. (Optional) To monitor the status of the migration, do the following:

   a. From vCenter, click **Home** and then click **AWS Management Portal**.
   b. Expand the region for the instance, select the environment, and then click the **VM-to-EC2 Migrations** tab.
   c. Find the entry with the import task ID or queued task ID that you noted earlier. The ID of the instance is shown in the **Instance ID** field.
7. To start the EC2 instance after the migration has completed, expand the environment, expand **Imported Instances**, select the instance, and then click the **Summary** tab. The ID of the instance should be the instance ID that you noted from the **VM-to-EC2 Migrations** tab. On the **Getting Started** tab, click **Start instance**.

Backing Up Your Instance

After you start an instance, it runs until it is terminated. If your instance is terminated, you can't connect to or recover the instance. To ensure that you can start a new instance with the same software as an migrated instance if needed, create an Amazon Machine Image (AMI) from the instance, and then create a template that specifies the AMI.

To create an AMI, you must use the Amazon EC2 console or command line tools. For information about creating an AMI using Amazon EC2, see the following topics in the *Amazon EC2 User Guide*.

Platform	Root Volume	Topic
Linux	EBS	Creating an Amazon EBS-Backed Linux AMI

Platform	Root Volume	Topic
Linux	instance store	Creating an Instance Store-Backed Linux AMI
Windows	EBS	Creating an Amazon EBS-Backed Windows AMI
Windows	instance store	Creating an Instance Store-Backed Windows AMI

For information about creating a template so that you can launch instances from the AMI that you've created from your migrated instance, see Managing Templates (p. 31).

Exporting a Migrated EC2 Instance

To export an EC2 instance that you previously migrated from a VM, use the management portal in vCenter. The process for exporting an instance creates an OVA file and stores it in an Amazon S3 bucket in your AWS account.

If you have not previously exported an EC2 instance using vCenter, you must first specify the name that we will use for the S3 buckets that we create for instance export. AWS creates one S3 bucket in each region for this purpose, with a name that follows the form `export-to-s3-`*`name`*`-`*`region`*.

Requirements

- You must be an administrator of the management portal to export an EC2 instance.
- You can configure instance export using the AWS credentials of either an administrator or an IAM user. To allow an IAM user to complete these steps, verify that the user has the permissions described in Creating the Required Accounts and Users (p. 6).

Limits

- There is a limit of five concurrent export tasks per region.
- You can't export an instance that is currently being exported.

To prepare for instance export

1. Open the AWS Management Portal for vCenter setup console.
2. On the **AWS Management Portal for vCenter** page, click **Configure Instance Export**, and then click **Create New**.
3. On the **Configure Instance Export** page, do the following:

   a. Complete the bucket name in **S3 bucket names** as prompted.
   b. Click **I agree that AWS Management Portal for vCenter may do the following on my behalf**.
   c. Click **Create**.

To export a migrated instance

1. From vCenter, click **Home** and then click **AWS Management Portal**.
2. From the dashboard, expand the region, the environment, and the template for the instance.
3. Select the instance.
4. On the **Getting Started** tab, click **Export instance to S3**.

5. In the **Export instance to S3** dialog box, enter a name for the OVA file in **S3 object file prefix** and then click **Export**.

   After the export begins, we display the export task ID. Note this ID if you want to monitor the status of the export task.

6. (Optional) To monitor the status of the export process, select the environment for the instance and then click the **EC2-to-S3 Migrations** tab. This tab displays all instance export tasks from the last seven days. Find the task with the export task ID that you noted earlier. If you need to cancel the export task while it is in progress, right-click the row, click **Cancel Export Task**, and click **Continue** when prompted for confirmation.

7. To access the OVA file after the export process has completed, do the following:

   a. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.

   b. From the navigation bar, select the region that contains the EC2 instance that you exported. The OVA file is stored in an S3 bucket in the same region as the EC2 instance.

   c. From the **Buckets** pane, select the bucket for your exported instances (`export-to-s3-`*`name`*`-`*`region`*) and then select the OVA file.

   d. Click **Actions** and then click **Download**. Follow the directions to complete the download.

Alternatively, you can export an EC2 instance using the Amazon EC2 CLI instead of using the connector. For more information, see Exporting Amazon EC2 Instances in the *Amazon EC2 User Guide*.

Troubleshooting Migration

Error: Additional permissions are required to migrate multidisk virtual machines

When migrating a virtual machine, you receive the error "To migrate a virtual machine with more than one disk, log into the management portal setup page and grant the additional permissions required by the VM Import/Export service."

Use the following procedure to grant the required permissions:

1. Open the AWS Management Portal for vCenter setup console.
2. If you see an error message indicating that your Import service role is missing, click **Fix Error**.
3. (Optional) Click **View Policy** to review the policy for the import service role.
4. Click **I agree that AWS Management Portal for vCenter may create the above roles on my behalf**.
5. Click **Save**.

Error: Connector is unable to reach ESX host

You receive the following error when migrating a virtual machine: "Connector is unable to reach ESX host [*hostname*] to migrate virtual machine [*name*]".

If the hostname specified in the error message is not the fully-qualified domain name of an ESX host, use the following procedure to configure the DNS suffix search list so that connector can append the suffix and resolve the ESX hostname:

1. Locate the connector VM in the vSphere client, right-click it, and select **Open Console**.
2. Log in as ec2-user. For more information, see Logging into the Virtual Machine Console (p. 42).
3. Run the **sudo setup.rb** command. This command displays the following menu:

```
Choose one of the following options
```

```
1. Reset password
2. Reconfigure network settings
3. Restart services
4. Factory reset
5. Delete unused upgrade-related files
6. Enable/disable SSL certificate validation
7. Display connector's SSL certificate
8. Generate log bundle
9. Exit
Please enter your option [1-9]:
```

4. Type 2, and then press Enter. The command displays the following menu:

```
Reconfigure your network:
1. Renew or acquire a DHCP lease
2. Set up a static IP
3. Set up a web proxy for AWS communication
4. Set up a DNS suffix search list
5. Exit
Please enter your option [1-5]:
```

5. Type 4, and then press Enter. The command displays the current DNS suffix search list. Follow the directions to update the search list to include the domain name of the ESX host from the error message.

Connector can't validate the certificates of the host

By default, the connector validates the certificates of all entities that it communicates with over HTTPS, including vCenter and ESXi servers. This is essential to prevent man-in-the-middle attacks. However, if you are migrating a virtual machine from ESX version 4.1 or earlier to Amazon EC2, the connector can't validate the certificates of the host, so the migration fails.

To work around this problem, you can do one of the following:

*   **Option 1**: Update to ESX 5.0 or later.
*   **Option 2**: Disable ESX certificate validation, migrate the virtual machine, and then re-enable ESX certificate validation as follows:

    1. From your web browser, open the connector management console (https://*ip_address*/, where *ip_address* is the IP address of the management console) and log in using your password.
    2. Click **Register the Connector**.
    3. On the **Register Plugin** page, under **ESX SSL certificate options**, click **Ignore any ESX certificate errors**, and then click **Register**.

        Important
        We recommend that you keep ESX certificate validation enabled unless you are migrating virtual machines from ESX 4.1 or earlier.

    4. When you have finished migrating the virtual machine, return to the **Register Plugin** page of the connector management console, click **Trust vCenter to validate ESX certificates**, and then click **Register**.

Managing the AWS Connector for vCenter

You can manage the connector using the connector management console and the connector CLI.

Starting with connector version 2.4.0, AWS collects metrics about the performance, usage, and customization of your connector so that we can make it more stable and secure.

> **Note**
> We recommend using AWS Server Migration Service (SMS) to migrate VMs from a vCenter environment to AWS. SMS automates the migration process by replicating on-premises VMs incrementally and converting them to Amazon machine images (AMIs). You can continue using your on-premises VMs while migration is in progress. For more information about AWS SMS, see AWS Server Migration Service.

Contents

Note that the procedures on this page are written for version 2.1.0 and later of the connector. If the version information in the upper-right corner of the connector management console is **Version: 2.0.0**, download the PDF file Managing the Connector for directions written for version 2.0.0 of the connector.

Accessing the Management Console

To access the management console, go to https://*ip_address*/, where *ip_address* is the IP address of the connector management console that you saved when you deployed the connector virtual appliance.

Logging into the Virtual Machine Console

You can use the connector CLI from the connector virtual machine console. To access the virtual machine console, locate the connector VM in the vSphere client, right-click it, and select **Open Console**.

The default user is ec2-user and the default password is ec2pass.

We recommend that you change the password after you have logged in. To change the password, use the following command:

```
passwd new_password
```

> **Important**
> Note that if you use the command `sudo passwd` it will modify the password for `root`, not the password for `ec2-user`.

Resetting the Connector Password

If you forget the password that you use to log in to the connector setup console, you can reset the password using the connector CLI.

To reset your password using the connector CLI

1. Locate the connector VM in the vSphere client, right-click it, and select **Open Console**.
2. Log in as ec2-user. For more information, see .
3. Run the **sudo setup.rb** command. This command displays the following menu:

```
Choose one of the following options
1. Reset password
2. Reconfigure network settings
3. Restart services
4. Factory reset
5. Delete unused upgrade-related files
6. Enable/disable SSL certificate validation
7. Display connector's SSL certificate
8. Generate log bundle
9. Exit
Please enter your option [1-9]:
```

4. Type `1`, and then press Enter. Follow the onscreen directions. Note that in general, you should not change the vCenter IP/hostname, you should use the same vCenter to authenticate.

Rotating the Keys

We recommend that you rotate these keys periodically.

The AMP-connector key is shared between the management console and the on-premises connector and is used to establish trust between these entities.

To rotate the AMP-connector key

1. Open the AWS Management Portal for vCenter setup console.
2. On the **AWS Management Portal Setup** page, expand the **AMP-Connector Key** pane and then click **Edit**.
3. On the **Create an AMP-Connector Key** page, select **Create a new AMP-Connector key**.
4. Enter a name for the key and then click **Create**.
5. On the **Review Your Configuration** page, click **Download Configuration**. Save this file to a safe location. You'll need it to complete the connector deployment process.

6. Click **Finish**.

The connector encryption key is used to encrypt sensitive information (such as account credentials) that is local to the connector.
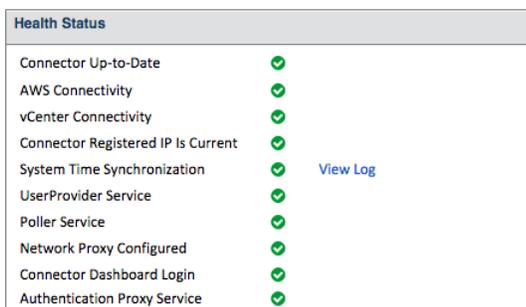
To rotate the connector encryption key

1. Using a web browser, open the connector management console.
2. From the connector management console, click **Rotate encryption key**.
3. In the **Rotate encryption key** dialog box, enter a password for the connector and then click **Rotate**.

Monitoring the Connector

The connector enables you to monitor its health using the management console.

To monitor the connector using the management console

1. Using a web browser, open the connector management console.
2. Locate the **Health Status** pane.

3. Check whether there are any failures. If there is a failure, click **View Error Log** for more information.

   Connector Up-to-Date

   Indicates whether you are using the current version of the connector. If you see a warning icon, there is an upgrade available; click **What's new?** to learn more. If you see an error icon, the connector has been recalled and there is a downgrade available; click **What will be fixed?** to learn more.

   AWS Connectivity

   Verifies that the connector can access AWS using the credentials you specified when you configured the connector. If there are errors, click **View Error Log**.

   vCenter Connectivity

   Verifies that the connector can access vCenter using the credentials you specified when you configured the connector. If there are errors, click **View Error Log**.

   Connector Registered IP Is Current

   Indicates whether the IP address used to register the connector is valid.

   System Time Synchronization

   Verifies that the time of the current system and the host are in sync. If there are errors, click **View Error Log**. For more information, see Configuring Time Synchronization (p. 4).

UserProvider Service

Enumerates vCenter users. If there are errors, click **View Error Log**.

Poller Service

Monitors the status of VMs that you migrate to Amazon EC2. If there are errors, click **View Error Log**. If the error is that the service hasn't refreshed, try restarting services, as described in Troubleshooting Upgrades (p. 47).

Network Proxy Configured

Indicates whether you are connected using a proxy. If you are not using a network proxy, this item is not present.

Connector Dashboard Login

Indicates whether there are attempts to log in to the connector with an incorrect password. After 20 attempts to log in with an incorrect password, the connector is locked down.

Authentication Proxy Service

Indicates that you are using the federation authentication proxy in the connector to validate user credentials when they log into AWS Management Portal for vCenter. If you are using SAML-based authentication, this item is not present.

Reporting a Problem to AWS

Use the following procedure to report a problem with the connector to AWS. We recommend that you send us your connector logs. Sending your logs is secure, and it enables us to provide you with better support.

To report an issue to AWS

1. From your web browser, go to https://*ip_address*/, where *ip_address* is the IP address of the connector management console.
2. Log in to the connector using your password.
3. Under **Support Links**, click **Report a problem to AWS**.
4. In the **Report a problem to AWS** dialog box, do the following:

   a. Select an issue from the list of common issues provided, or 'Other' if your issue is not listed.

   b. Describe the issue in the text box.

   c. To include your connector logs, select **I agree to send my logs to Amazon Web Services**.

   d. Click **Send**.

Updating the AWSConnector Policy

If you installed a version of AWS Connector for vCenter earlier than 2.4.0, you must update the policies used by the IAM users that you created during the setup process as follows. This ensures that these users are granted the access to AWS that is now required to migrate a VM.

To update the AWSConnector policy

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, click **Users**.
3. Select the user.

4. On the **Permissions** tab, click **Remove Policy** for the `AWSConnector` policy. When prompted for confirmation, click **Remove**.

5. Click **Attach Policy**.

6. Select the check box next to the **AWSConnector** policy.

7. Click **Attach Policy**.

General Troubleshooting

If you need to download and review the log files

If you need to troubleshoot issues with the connector, you can download the debug log files as follows:

1. Using a web browser, open the connector management console.

2. From the dashboard, click **Download Debug Log Bundle**.

3. Download and review the log files.

If AWS Management Portal for vCenter is not showing up in vSphere Web Client

1. Log out of vSphere Web Client and then log back in.

2. If the management portal is still not showing up, re-register the connector as follows:

   a. Using a web browser, open the connector management console.

   b. From the dashboard, click **Register the Connector**.

   c. Follow the directions to complete the registration wizard.

   d. Log out of vSphere Web Client and then log back in.

3. If the management portal is still not showing up, restart the service for the connector, as described in the procedure for "If the connector isn't responding" below, and then re-register the connector as described in the previous step.

If the connector isn't responding

1. You can restart the services for the connector using the connector CLI as follows:

   a. Locate the connector VM in the vSphere client, right-click it, and select **Open Console**.

   b. Log in as ec2-user. For more information, see .

   c. Run the **sudo setup.rb** command. This command displays the following menu:

```
Choose one of the following options
1. Reset password
2. Reconfigure network settings
3. Restart services
4. Factory reset
5. Delete unused upgrade-related files
6. Enable/disable SSL certificate validation
7. Display connector's SSL certificate
8. Generate log bundle
9. Exit
Please enter your option [1-9]:
```

   d. Type 3, and then press Enter. Follow the onscreen directions.

2. Alternatively, you can reboot the host computer itself. Locate the connector in the vSphere client inventory tree, right-click it, and then select **Power > Restart Guest**.

3. If restarting the services or rebooting doesn't fix the problem, you can perform a factory reset as follows:

    Warning
    Performing a factory reset should be a last resort. You'll need to configure the connector after the factory reset is complete.

    a. Locate the connector VM in the vSphere client, right-click it, and select **Open Console**.
    b. Log in as ec2-user. For more information, see .
    c. Run the **sudo setup.rb** command. This command displays the following menu:

    ```
    Choose one of the following options
    1. Reset password
    2. Reconfigure network settings
    3. Restart services
    4. Factory reset
    5. Delete unused upgrade-related files
    6. Enable/disable SSL certificate validation
    7. Display connector's SSL certificate
    8. Generate log bundle
    9. Exit
    Please enter your option [1-9]:
    ```

    d. Type 4, and then press Enter. Follow the onscreen directions.
    e. After the factory reset is complete, it's as if you have just downloaded the OVA file and installed it. You must configure the connector again. For more information, see .

Troubleshooting Upgrades

If an error occurs during an upgrade

1. From the management console, check whether there are any failures in the **Health Status** pane. If there is a failure, attempt to resolve the issue. For more information, see .
2. Refresh the page and retry the upgrade.
3. If the error persists, send debug logs to AWS. For more information, see .

If an upgrade continues for a long time

If you have launched a manual upgrade of connector version 2.4.*x* from the management console, the upgrade process can take a long time to finish. This is because we are making security upgrades to the connector.

1. If the upgrade is still in progress after 20 minutes, refresh your browser. If the page is down, the upgrade process might not have finished; try refreshing again after another 10 minutes.
2. When prompted by your browser, accept the new certificates for connector.
3. Log in to the connector.

If the connector is unresponsive after an upgrade

1. If the connector is still unresponsive after 30 minutes, reboot the connector appliance.
2. If the connector remains unresponsive, contact AWS Support for further assistance.

Installing a Trusted SSL Certificate

The first time that you power on the connector appliance, it automatically generates a self-signed certificate based on its IP address. Because this is a self-signed certificate, your web browser notifies you that it is an untrusted certificate the first time you visit the connector management console. We recommend that you validate this certificate before you trust it, and then replace the certificate by installing an SSL certificate signed by a trusted certificate authority (CA) on your connector, as shown in the following procedure. After you do so, you will make subsequent connections to the connector using the new certificate.

To install an SSL certificate on your connector

1. Before uploading a trusted certificate to the connector, we recommend that you ensure that communication between your computer and the connector over the network is secure. For more information, see Validating an Untrusted SSL Certificate (p. 48).

2. Create a private key and obtain a corresponding trusted certificate in PEM format. The recommended way to do this is as follows:

   a. Create the private key and certificate signing request (CSR) using tools such as the openssl tools. You must specify the IP address of the connector. If you've set up a DNS hostname that resolves to the IP address of the connector, you must also specify the DNS hostname of the connector.

   b. Submit the CSR to your CA.

   c. Wait for the CA to send you the trusted certificate.

3. Package the private key and trusted certificate into a PKCS#12 file with a passphrase as follows:

   ```
   openssl pkcs12 -export -inkey my-private-key.pem -in my-certificate.pem -out my-
   passphrase.p12 -passout pass:passphrase
   ```

4. Open the management console.

5. In the **Actions** pane, click **Upload security certificate**.

6. In the **Upload Security Certificate** dialog box, click **Choose file** and select your PKCS 12 file. Enter the passphrase and then click **Upload**.

Each SSL certificate has a validity period. You must replace a certificate before its validity period ends. To replace a certificate, you must create and upload a new certificate.

Validating an Untrusted SSL Certificate

The first time that you power on the connector appliance, it automatically generates a self-signed certificate based on its IP address. The connector presents your browser with this certificate to identify itself and encrypt the connection. This certificate helps your browser determine whether this site is actually the site that it claims to be. Because this is a self-signed certificate, your web browser notifies you that it is an untrusted certificate the first time you visit the connector management console. (Check the error message in your browser for details.) We recommend that you validate this certificate before you trust it.

If the IP address shown in the SSL certificate for the connector is different than the current IP address of the connector, you should restart the services on the connector, which regenerates the certificate using the current IP address. For more information, see Restart Services (p. 46).

You can validate the untrusted certificate by viewing the certificate details as follows, and comparing them against the untrusted certificate.

To view the connector certificate

1. Locate the connector VM in the vSphere client, right-click it, and select **Open Console**.
2. Log in as ec2-user. For more information, see .
3. Run the **sudo setup.rb** command. This command displays the following menu:

```
Choose one of the following options
1. Reset password
2. Reconfigure network settings
3. Restart services
4. Factory reset
5. Delete unused upgrade-related files
6. Enable/disable SSL certificate validation
7. Display connector's SSL certificate
8. Generate log bundle
9. Exit
Please enter your option [1-9]:
```

4. Type 7, and then press Enter.

Uninstalling the Connector

If you need to uninstall the connector, complete the following steps.

To uninstall the connector

1. Using a web browser, open the connector management console.
2. From the dashboard, click **Unregister the Connector**.
3. In the **Unregister the Connector** dialog box, enter the user name and password, and then click **Unregister**.
4. Sign in to vCenter.
5. Locate the connector in the vSphere client inventory tree, right-click it, and select **Power > Power Off**. Right-click the template again and select **Delete from Disk**.

Document History

The following table describes the important changes to this documentation.

Change	Description	Release Date
AWS Connector for vCenter version 2.7.0	vSphere Web Client support: You can now use AWS Connector for vCenter with vSphere Web Client 5.5 and 6.0. You must register your connector after the upgrade. For more information, see Re-register your connector to use it with vSphere Web Client. (p. 46) Improved error reporting to AWS: When you send logs to AWS, you can provide a description of the issue you are troubleshooting. For more information, see Reporting a Problem to AWS (p. 45). Improved VM migration: When you migrate a VM, any CD or DVD drives attached to the VM are excluded automatically.	January 20, 2016
AWS Connector for vCenter version 2.6.0	You can now use connector to migrate virtual machines with more than one virtual disk to Amazon EC2. This feature may require that you grant additional permissions. For more information, see Additional permissions are required to migrate multidisk virtual machines (p. 40).	October 28, 2015
Added support for exporting a migrated EC2 instance	After you migrate a VM to Amazon EC2, you can export the instance if needed. This process creates an OVA file and stores it in an S3 bucket in your AWS account. For more information, see Exporting a Migrated EC2 Instance (p. 39).	August 26, 2015
AWS Connector for vCenter version 2.5.0	vCenter 6.0 support: You can use VMware vCenter 6.0 from the vSphere Client for desktop. New region support: You can create resources and migrate VMs to Amazon EC2 in the Europe (Frankfurt) region. Trusted SSL certificates: You can upload an SSL certificate to your connector so that your browser can verify the site. For more information, see Installing a Trusted SSL Certificate (p. 48). DNS suffix configuration: You can configure the DNS suffix search list through the CLI.	July 22, 2015
AWS Connector for vCenter version 2.4.x	Automatic upgrades: You can receive automatic upgrades for the connector. VM import: If the connector reaches its limit on the number of active import tasks, it queues additional import tasks until an active import task completes successfully or is canceled. For more information, see Migrating Your Virtual Machine to Amazon EC2 Using AWS Connector for vCenter (p. 36). Verify untrusted SSL certificates: You can display the SSL certificate of the connector from the setup CLI so that you can	March 05, 2015

Change	Description	Release Date
	manually verify the certificate that the management console presents to your browser. For more information, see Validating an Untrusted SSL Certificate (p. 48). Debug logs: You can securely send connector logs to AWS. For more information, see Reporting a Problem to AWS (p. 45).	
Added support for configuration reset and managing existing EC2 instances	If you want to change the authentication provider that you used to set up AWS Management Portal for vCenter, you can return to the setup program and reset the trust relationship. You can manage your EC2 instances that you created outside AWS Management Portal for vCenter using AWS Management Portal for vCenter.	October 03, 2014
Added support for the connector as an authentication provider	Starting with version 2.1.0 of the connector, you can choose the connector as the authentication provider for the management portal. The initial release of AWS Management Portal for vCenter included version 2.0.0 of the connector, which requires that you use an identity provider (IdP) that supports SAML 2.0 as the authentication provider. For more information, see Installing and Configuring AWS Management Portal for vCenter (p. 3).	August 20, 2014
Added support for default environments	Default environments enable you manage EC2 instances that were created for your AWS account using tools other than the management portal. For more information, see Managing Environments (p. 26).	August 20, 2014
Initial release	The initial release of the *AWS Management Portal for vCenter User Guide*.	May 30, 2014