Managing Amazon Cloud Accounts

Configuring Amazon Cloud Accounts

Step 1 In Amazon EC2, create a public cloud account.

Step 2 Note the following information about the Amazon account from the Amazon Web Services (AWS) management portal:

- AWS access key
- AWS secret access key
- AWS region

Step 3 In AWS, add the desired operating system images to the account.
See Amazon Machine Images (AMI).

Step 4 If you connect through a proxy server, configure the proxy server settings in the `inframgr.env` file in the Cisco UCS Director VM.
See Public Cloud Accounts and Proxy Servers.

Step 5 In Cisco UCS Director, create a virtual account for the Amazon cloud account.
See Adding an Amazon Cloud Account, on page 2.

Step 6 Create an Amazon deployment policy.
See Creating an Amazon Deployment Policy, on page 3.

Step 7 (Optional) If you want to set up a chargeback for end users, define a public cloud cost model in the Cisco UCS Director chargeback module.
For more information, see the Cisco UCS Director Administration Guide.

Step 8 Create a virtual data center (vDC) for the Amazon cloud account.
For more information, see the Cisco UCS Director Administration Guide.

Step 9 Add a catalog for each operating system image that you want to make available to end users.
For more information, see the Cisco UCS Director Administration Guide.

Step 10 In the End User Portal, provision a VM through a service request.
For more information, see the Cisco UCS Director Administration Guide or the Cisco UCS Director End User Portal Guide.

Adding an Amazon Cloud Account

Before You Begin

- Create a public cloud account in Amazon EC2.
- Create and upload any desired operating system images to the Amazon account.
- If you connect through a proxy server, configure the proxy server settings in the `inframgr.env` file.

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Cloud** screen, choose **AWS-EC2** from the **Cloud Type** drop-down list and complete the following fields:

a) In the **Cloud Name** field, enter a unique name for this account.
b) In the **EC2 Account Number** field, enter an account number for this account.
c) In the **AWS Access Key** field, enter the access key for this account from the AWS management portal.
d) In the **AWS Secret Access Key** field, enter the secret access key for this account from the AWS management portal.
e) From the **AWS EC2 Region** drop-down list, choose the region where the public cloud is located.
You must choose the same region as the Amazon account has in the AWS management portal.

f) (Optional) In the **Description** field, enter a description of the public cloud.
g) (Optional) In the **Contact Email** field, enter an email address for the contact person.
h) In the **Location** field, enter the location of the public cloud.
i) In the **Service Provider** field, enter the name of the service provider responsible for the public cloud.

Step 5 Click **Add**.

Cisco UCS Director tests the connection to the Amazon EC2 cloud. If that test is successful, it adds the Amazon cloud account. This discovery process and inventory may take a few minutes.

Creating an Amazon Deployment Policy

The Amazon deployment policy determines the actions that are performed when a user creates a VM in the cloud through the End User Portal.

Before You Begin

Create an Amazon cloud account.

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Amazon Deployment Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Policy** screen, do the following:

a) Enter a unique name and description for the policy.
The policy name is used when you define the vDC.

b) From the **Keypair Type** drop-down list, choose the type of policy used to manage AWS key pairs.
In the End User Portal, when a user requests an application or VM, this policy is used to either generate a new key pair or reuse an existing key pair. The user who makes the request is sent a copy of the key through email. This policy can be one of the following:

- **Unique—**Generates a unique key pair for each VM.
- **Group Share—**Assigns all VMs in a security group to the same key pair.
- **Custom—**Uses the key pair you enter in the **Keypair Name** field for all VMs.

c) If desired, check the **Enable CloudWatch** check box.
If checked, Amazon CloudWatch monitoring services are enabled during the deployment of all VMs that are provisioned through this policy. An administrator can enable or disable CloudWatch on a VM at any time.

d) In the **Security Group** field, enter the name of the security group to use for VMs created with this policy.

e) In the **Firewall Specifications** field, enter the list of firewall rules for the Amazon cloud account.
You can enter multiple rules and separate them with a semi-colon (;).

Each firewall rule must include the following: *protocol*,*port_range_start*,*port_range_end*,*source_CIDR*.

For example, the following is a valid pair of firewall rules: `tcp,80,80,0.0.0.0/0;tcp443,443,0.0.0.0/0`

f) From the following drop-down lists, choose the type (size) of instance to which the relevant images can be deployed in Amazon EC2:

- **32bit VM Instance Type** drop-down list
- **64bit VM Instance Type** drop-down list

For more information about instance types, see Amazon EC2 Instances.

g) In the **User Data** field , enter the data required for a parameterized launch of an Amazon EC2 instance.
This data is made available to those instances in addition to the standard metadata. If you do not want to use the parameterized launch feature, leave this field blank. For more information about parameterized launches and the types of data permitted, see Introduction to Parameterized Launches.

h) Click **Add**.

Updating Images in an Amazon Cloud Account

Cisco UCS Director does not host operating system images for an Amazon cloud account. The images must already exist in AWS. Then Cisco UCS Director performs an inventory collection from the AWS account to make them available for catalogs.

Note If you do not see any images for the Amazon cloud account, verify that the region in the account is the same as the region for the Amazon account in the AWS management portal.

Step 1 In AWS, add or update the images to the Amazon account.

Step 2 Log into Cisco UCS Director.

Step 3 Choose **Virtual** > **Compute**.

Step 4 On the **Compute** page, choose the cloud.

Step 5 On the **Compute** page, click **Polling**.
You can view the last time Cisco UCS Director performed an inventory collection for the account.

Step 6 If you updated or added a new image to the Amazon account after the last inventory collection, you can click **Request Inventory Collection** to perform one immediately.
By default, Cisco UCS Director performs an inventory collection every fifteen minutes.

Monitoring an Amazon Cloud Account

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 Click one of the following to monitor the Amazon cloud account:

Report Name	Description
Summary	This report allows you to monitor system inventory and lifecycle actions. It also gives you access to a wide array of tabular, graphical, and map reports that provide a view of trending data for the account.
vDCs	This report displays information about the vDCs associated with the account, including the group, type, lock state, and VMs.

Report Name	Description
VM Action Requests	This report displays information about the current status of all VM action requests, including the action requested, the user who requested it, and the status of the request.
Events	This report displays information about all events related to the account, including severity, time of the event, user who initiated it, type, description, instance name, and host name.
VMs	This report displays information about all VMs created in the account, including VM ID, instance name, IP address, image ID, monitor state, power status, group name, provisioned time, scheduled termination, if any, and the date and time of the last status update.
Images	This report displays information about all images available to the account, including the image ID, guest operating system, platform, architecture, image location, and root device type.
Deleted VMs	This report displays information about any VMs that have been deleted from the account, including VM ID, instance name, IP address, image ID, and architecture.

Step 4 If desired, you can click the report icons to customize the table columns, filter the results, or export a report of the current table contents.
For more information, see the Cisco UCS Director Administration Guide.

Viewing Reports about an Amazon Cloud Account

In addition to these reports, you can also create Cloudsense Analytics for VMs and other items, as described in the Cisco UCS Director Administration Guide.

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 Click one of the following to view reports about the Amazon cloud account:

Report Name	Description
Summary	This report allows you to monitor system inventory and lifecycle actions. It also gives you access to a wide array of tabular, graphical, and map reports that provide a view of trending data for the account.

Report Name	Description
Top 5 Reports	This report displays information about the top five VMs and vDCs in several categories, including memory usage, CPU usage, and disk usage.
Map Reports	This report provides reports as maps, including a CPU utilization map, memory utilization map, and deleted VMs map.
More Reports	This report provides trending and instant reports for a specified duration, including reports on VMs, CPUs, CPU usage, disk reads and writes, and network usage.

Step 4 For some reports, you can click the icons to customize the table columns, filter the results, or export a report of the current table contents.
For more information, see the Cisco UCS Director Administration Guide.