Cisco UCS Director Public Cloud Management Guide, Release 6.5

First Published: 2017-07-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Preface v

Audience v

Conventions v

Related Documentation vii

Documentation Feedback vii

Obtaining Documentation and Submitting a Service Request vii

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information for this Release 1

CHAPTER 2

Overview 3

About Public Cloud Support 3

Supported Public Clouds 3

Public Cloud Management Tasks You Can Perform in Cisco UCS Director 3

Public Cloud Orchestration Tasks 4

Public Cloud Accounts 4

Public Cloud Accounts and Proxy Servers 5

Guidelines and Limitations for Public Cloud Accounts with Proxy Servers 5

Accessing a Public Cloud Account Through a Proxy Server 5

Public Cloud Deployment Policies 6

CHAPTER 3

Managing Amazon Cloud Accounts 7

Configuring Amazon Cloud Accounts 7

Adding an Amazon Cloud Account 8

Creating an Amazon Deployment Policy 9

Updating Images in an Amazon Cloud Account 10

Monitoring an Amazon Cloud Account 10

Viewing Reports about an Amazon Cloud Account 11

CHAPTER 4 Managing Rackspace Cloud Accounts 13

Steps to Configure Rackpace Cloud Accounts 13

Adding a Rackspace Cloud Account 14

Creating a Rackspace Deployment Policy 15

Updating Images in a Rackspace Cloud Account 16

Monitoring a Rackspace Cloud Account 16

Viewing Reports about a Rackspace Cloud Account 17

Preface

- Audience, page v
- Conventions, page v
- Related Documentation, page vii
- Documentation Feedback, page vii
- Obtaining Documentation and Submitting a Service Request, page vii

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.

Text Type	Indication
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

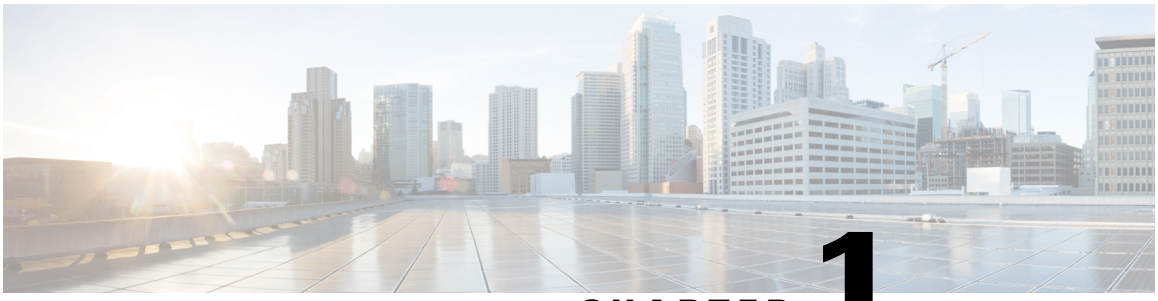
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

New and Changed Information for this Release

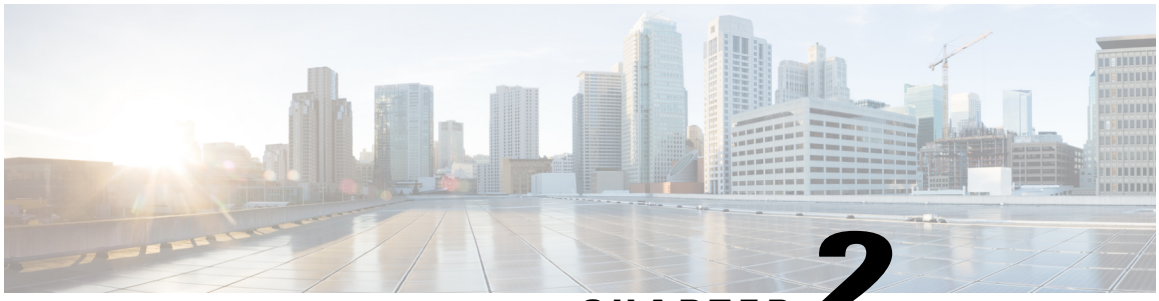
This chapter contains the following sections:

- New and Changed Information for this Release, page 1

New and Changed Information for this Release

No significant changes were made to this guide for the current release.

New and Changed Information for this Release



CHAPTER 2

Overview

- About Public Cloud Support, page 3
- Supported Public Clouds, page 3
- Public Cloud Management Tasks You Can Perform in Cisco UCS Director, page 3
- Public Cloud Orchestration Tasks, page 4
- Public Cloud Accounts, page 4
- Public Cloud Accounts and Proxy Servers, page 5
- Public Cloud Deployment Policies, page 6

About Public Cloud Support

You can add, manage, and monitor supported public cloud accounts in Cisco UCS Director.

After you have added and configured a public cloud, end users can provision virtual machines (VMs) in the End User Portal.

Supported Public Clouds

Cisco UCS Director supports the following public clouds:

- Amazon Elastic Compute Cloud (Amazon EC2)
- Rackspace Public Cloud

Public Cloud Management Tasks You Can Perform in Cisco UCS Director

You can use Cisco UCS Director to provision and the following for each supported public cloud account:

- Connect to the public cloud account

- View images available in that public cloud account
- Provision a VM in that public cloud
- Monitor the public cloud account, including the system inventory, lifecycle actions, VMs in the cloud, VM action requests, images, and events
- Generate tabular, graphical, and map reports for the public cloud account, including memory usage, disk usage, and other trending and statistical data

Public Cloud Orchestration Tasks

Cisco UCS Director includes orchestration features that allow you to automate some Amazon VM-related tasks in one or more workflows. For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.

Location of Orchestration Tasks

A complete list of the public cloud orchestration tasks is available in the Workflow Designer, in the Task Library and the **Amazon VM** folder. The Task Library includes a description of the orchestration tasks, and can be accessed from the following locations in Cisco UCS Director:

- **Policies** > **Orchestration** > **Workflows**
- `http://IP_address/app/cloudmgr/onlinedocs/cloupiaTaskLib.html` where *IP_address* is the IP address of Cisco UCS Director.

Types of Orchestration Tasks

The Amazon VM orchestration tasks include tasks for VM provisioning and limited support for VM lifecycle management, such as the following:

- Power action, including power on, power off, reboot, terminate, and enable or disable Cloudwatch monitoring
- Volume management, including create, delete, and attach and detach volume to instance

Public Cloud Accounts

You need to create a virtual account for each public cloud that you want to manage through Cisco UCS Director. For example, each Amazon cloud account represents a public cloud created through Amazon EC2.

Note You must register an account with a supported public cloud provider before you can add the account to Cisco UCS Director.

Public Cloud Accounts and Proxy Servers

Guidelines and Limitations for Public Cloud Accounts with Proxy Servers

If you need to access a public cloud account through a proxy server, consider the following guidelines and limitations:

- You must configure the proxy server in your Java Virtual Machine (JVM) before you add the account. If you do not, the connection test will fail.
- For the proxy settings to work, Cisco UCS Director must be synchronized with the system time (host) or NTP server for the DMZ. You can configure time synchronization through the Time Sync option in the Shelladmin. For more information, see the Shell Guide.
- After you apply a patch and upgrade Cisco UCS Director, you must reconfigure the proxy settings in the `inframgr.env` file.

Accessing a Public Cloud Account Through a Proxy Server

Before You Begin

You must know the following:

- Name of the proxy server
- Port used by the proxy server

Step 1 On the server or VM that hosts Cisco UCS Director, navigate to the `/opt/infra/bin` folder.

Step 2 Open the `inframgr.env` file.

Step 3 Add the following information for the proxy server to the `JVM_ARGS` section:

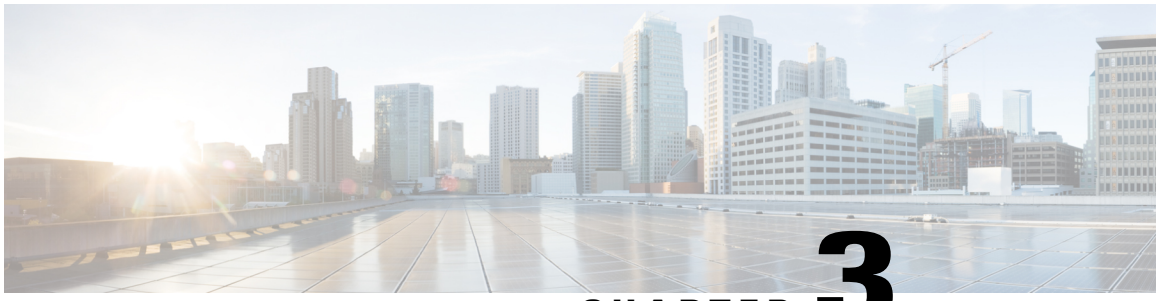
```
-Dhttp.useProxy=true -Dhttp.proxyHost=proxy_name
-Dhttp.proxyPort=proxy_port
```

The updated `JVM_ARGS` section should look like the following:

```
JVM_ARGS="-DSVC=$SVC -Xms$MEMORY_MIN -Xmx$MEMORY_MAX $REMOTE_DEBUG_OPTS -Djava.security.manager
-Djava.security.policy=security.policy
-DpreInitSchema=false -verbose:gc -Dfile.encoding=UTF-8 $JMX_OPTS -Dhttp.useProxy=true
-Dhttp.proxyHost=proxy_name
-Dhttp.proxyPort=proxy_port"
```

Public Cloud Deployment Policies

The public cloud deployment policies define the parameters that are required to provision VMs in the public cloud account. The configuration of these policies depends upon the type of public cloud account.



CHAPTER 3

Managing Amazon Cloud Accounts

- Configuring Amazon Cloud Accounts, page 7
- Adding an Amazon Cloud Account, page 8
- Creating an Amazon Deployment Policy, page 9
- Updating Images in an Amazon Cloud Account, page 10
- Monitoring an Amazon Cloud Account, page 10
- Viewing Reports about an Amazon Cloud Account, page 11

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, on page 5.

Step 5 In Cisco UCS Director, create a virtual account for the Amazon cloud account.
See Adding an Amazon Cloud Account, on page 8.

Step 6 Create an Amazon deployment policy.
See Creating an Amazon Deployment Policy, on page 9.

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**.

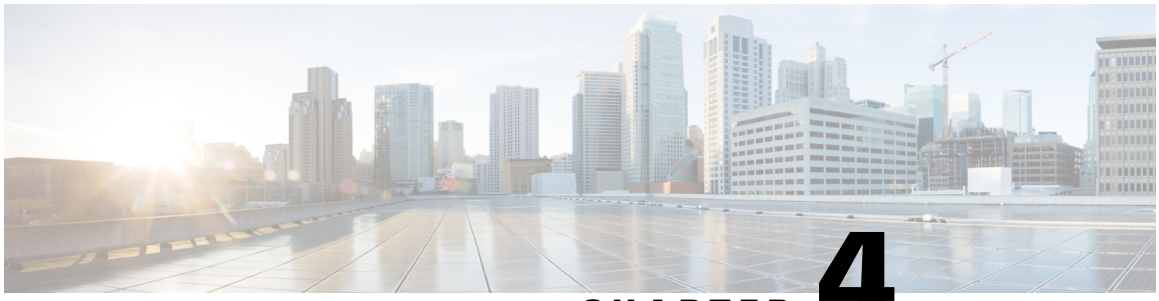
Step 2 On the **Compute** page, choose the cloud.

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.



CHAPTER 4

Managing Rackspace Cloud Accounts

- Steps to Configure Rackpace Cloud Accounts, page 13
- Adding a Rackspace Cloud Account, page 14
- Creating a Rackspace Deployment Policy, page 15
- Updating Images in a Rackspace Cloud Account, page 16
- Monitoring a Rackspace Cloud Account, page 16
- Viewing Reports about a Rackspace Cloud Account, page 17

Steps to Configure Rackpace Cloud Accounts

Step 1 In Rackspace, create a public cloud account.

Step 2 Note down the following information about the Rackspace account:

- Access key
- Location

Step 3 In Rackspace, add the desired operating system images to the account.

Step 4 If you connect through a proxy server, configure the proxy server settings in the `run.sh` file in the Cisco UCS Director VM.
See Public Cloud Accounts and Proxy Servers, on page 5.

Step 5 In Cisco UCS Director, create a virtual account for the Rackspace cloud account.
See Adding a Rackspace Cloud Account, on page 14.

Step 6 Create a Rackspace deployment policy.
See Creating a Rackspace Deployment Policy, on page 15.

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 Rackspace 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 a Rackspace Cloud Account

Before You Begin

- Create a public cloud account in Rackspace.
- Create and upload any desired operating system images to the Rackspace account.
- If you connect through a proxy server, configure the proxy server settings in the `run.sh` 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 **RackSpace-Cloud** 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 **User ID** field, enter the user ID for your Rackspace account.
c) In the **Access Key** field, enter the access key provided by the Rackspace account.
d) From the **Account Location** drop-down list, choose the location where the Rackspace account is located. You must choose the same location as the Rackspace account.
e) (Optional) In the **Description** field, enter a description of the public cloud.
f) (Optional) In the **Contact Email** field, enter an email address for the contact person.
g) In the **Location** field, enter the location of the public cloud.
h) 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 Rackspace cloud. If that test is successful, it adds the Rackspace cloud account. This discovery process and inventory may take a few minutes.

Creating a Rackspace Deployment Policy

The Rackspace 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 a Rackspace cloud account.

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

Step 2 On the **Service Delivery** page, click **Rackspace 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) In the **VM Name Template** field, enter the variables that will be used to automatically create the names of VMs in the Rackspace public cloud.
The following variables are permitted. You do not have to use all of these variables in the template. However, you muse enclose each variable as follows: `${VARIABLE}`.

- *CLOUD_NAME*—Cloud in which the VM is being deployed.
- *GROUP_NAME*—Group to which the VM belongs.
- *CATALOG_NAME*—Catalog item or entry.
- *USER*—ID of the user who requests the VM.
- *SR_ID*—ID of the service request.
- *COMMENTS*—Comments that are left by the user who requests the VM.
- *CLOUD_TYPE*—Type of public cloud, such as Rackspace or Amazon-EC2.
- *PROFILE_NAME*—Name of the deployment policy.
- *LOCATION*—Name of the location specified when the public cloud was created.
- *UNIQUE_ID*—A random ID, designed to make the name of the VM unique.

c) In the **Flavor** table, choose the flavor that will specify the size of the VM or instance in the public cloud.

d) Click **Add**.

Updating Images in a Rackspace Cloud Account

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

Step 1 In Rackspace, add or update the images to the Rackspace 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 Rackspace 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 a Rackspace 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 Rackspace 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.
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.

Report Name	Description
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 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 a Rackspace 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 In the right pane, click one of the following to view reports about the Rackspace 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.
Top 5 Reports	This report displays information on 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.