Red Hat CloudForms 4.0
Managing Providers

Managing your infrastructure, cloud, and containers providers and datastores

CloudForms Team

Red Hat CloudForms 4.0 Managing Providers

Managing your infrastructure, cloud, and containers providers and datastores

CloudForms Team
cloudforms-docs@redhat.com

Legal Notice

Abstract

This guide covers managing your infrastructure, cloud, and containers providers and datastores in CloudForms Management Engine.

Table of Contents

CHAPTER 1. INFRASTRUCTURE PROVIDERS

A provider is a server with software to manage multiple virtual machines that reside on multiple hosts. **Infrastructure → Providers** displays the providers in your environment.

The web interface uses virtual thumbnails to represent providers. Each thumbnail contains four quadrants by default, which display basic information about each provider.

1. Number of hosts

2. Management system software

3. Currently unused

4. Authentication status

Icon	Description
	Validated: Valid authentication credentials have been added.
	Invalid: Authentication credentials are invalid.
	Unknown: Authentication status is unknown or no credentials have been entered.

1.1. DISCOVERING PROVIDERS

Add providers to the CloudForms Management Engine environment by discovering them based on their IP addresses. This procedure demonstrates discovering Red Hat Enterprise Virtualization Manager providers. Providers must be running in order for the appliance to discover them.

1. Navigate to **Infrastructure → Providers**.

2. Click `Configuration`, then click `Discover Infrastructure Providers`.

3. Select the types of provider to discover.

Infrastructure Providers Discovery

Discover

☐ VMware vCenter

☐ Microsoft System Center VMM

☐ Red Hat Enterprise Virtualization Manager

> ❯ To authenticate to Red Hat Enterprise Virtualization hosts see Authenticating Red Hat Enterprise Virtualization Hosts.

> ❯ To authenticate to VMware vCenter hosts see Authenticating VMware vCenter Hosts.

4. Enter a Subnet Range of IP addresses starting with a From Address and ending with a To Address. The cursor automatically advances as you complete each octet.

Subnet Range

From Address	☐ . ☐ . ☐ . ☐
To Address	☐ . ☐ . ☐ . ☐

5. Click **Start**.

1.2. RED HAT ENTERPRISE VIRTUALIZATION MANAGER PROVIDERS

To use a Red Hat Enterprise Virtualization Manager provider, add it to the appliance and authenticate its hosts.

1.2.1. Adding a Red Hat Enterprise Virtualization Manager Provider

After initial installation and creation of a CloudForms Management Engine environment, add a Red Hat Enterprise Virtualization Manager provider to the appliance.

1. Navigate to **Infrastructure → Providers**.

2. Click ⚙ **(Configuration)**, then click ✚ **(Add a New Infrastructure Provider)**.

3. Enter the Name of the provider to add. The Name is how the device is labeled in the console.

4. Select Red Hat Enterprise Virtualization Manager from the Type list.

5. Enter the Host Name or IP address(IPv4 or IPv6) of the provider.

Important

The Host Name must use a unique fully qualified domain name.

6. Enter the API Port if your provider uses a non-standard port for access.

7. Select the appropriate Zone for the provider. By default, the zone is set to default.

8. In the Credentials area, under Default, provide the login credentials required for the Red Hat Enterprise Virtualization Manager administrative user:

    ≫ Enter the user name, admin@internal, in the Username field.

    ≫ Enter the password in the Password field.

    ≫ Confirm the password in the Confirm Password field.

    ≫ Click **Validate** to confirm CFME can connect to the Red Hat Enterprise Virtualization Manager.

9. Under C & U Database tab, provide the login credentials for the CloudForms user of the Red Hat Enterprise Virtualization Data Warehouse database:

    Note

    To obtain historical Capacity and Utilization (C & U) data for Red Hat Enterprise Virtualization Manager, you must create a CloudForms Management Engine user in the already-configured Red Hat Enterprise Virtualization Data Warehouse database. To create the user, see section "Data Collection for Red Hat Enterprise Virtualization 3.3 and 3.4" in the Deployment Planning Guide.

    For information on setting up the Data Warehouse service on the Manager, see the Red Hat Enterprise Virtualization Installation Guide.

    ≫ Enter the database user name in the Username field.

    ≫ Enter the user password in the Password field.

    ≫ Confirm the user password in the Confirm Password field.

    ≫ Click **Validate** to confirm CFME can connect to the database.

10. Click **Save**.

1.2.2. Authenticating Red Hat Enterprise Virtualization Hosts

After adding a Red Hat Enterprise Virtualization infrastructure provider, you must authenticate its hosts to enable full functionality.

1. Navigate to **Infrastructure → Providers**.

2. Click on a provider to display its summary screen.

3. On the summary screen, click Hosts in the Relationships information box to display the hosts on that provider.

4. Select the hosts to authenticate. You can select all hosts using the Check All option.

5. Click ⚙ **(Configuration)**.

6. Click ✏ **(Edit this item)**.

7. In the Credentials area, enter credentials for the following, as required:

    a. Default: This field is mandatory. Users should have privileged access such as, root or administrator.

    b. Remote Login: Credentials for this field are required if SSH login is disabled for the Default account.

    c. Web Services: This tab is used for access to Web Services in Red Hat Enterprise Virtuaization Manager.

    d. IPMI: This tab is used for access to IPMI.

8. Click **Validate**.

9. If editing multiple hosts:

    a. Select a host from the Select Host to validate against list.

    b. If required, enter credentials for Remote Login, Web Services, and IPMI in their respective tabs; click **Validate**.

    c. Select another host to validate each of these credentials against.

10. Click **Add**.

1.3. OPENSTACK INFRASTRUCTURE PROVIDERS

Enable an OpenStack Infrastructure provider by adding it to the appliance.

1.3.1. Adding an OpenStack Infrastructure Provider

After initial installation and creation of a CloudForms Management Engine environment, add an OpenStack Infrastructure provider to the appliance. CloudForms Management Engine supports operating with the OpenStack "admin" tenant. When creating an OpenStack Infrastructure provider in CloudForms Management Engine, select the OpenStack Infrastructure provider's admin user because it is the default administrator of the OpenStack admin tenant. When using the admin credentials, a user in CloudForms Management Engine provisions into the admin tenant, and sees images, networks, and instances that are associated with the admin tenant.

1. Navigate to **Infrastructure → Providers**.

2. Click ⚙ **(Configuration)**, then click ➕ **(Add a New Infrastructure Provider)**.

3. Enter the Name of the provider to add. The Name is how the device is labeled in the console.

4. Select OpenStack Platform Director from the Type list.

5. Enter the Host Name or IP address(IPv4 or IPv6) of the provider.

> **Important**
>
> The Host Name must use a unique fully qualified domain name.

6. Select the API Version of your Keystone service from the list. The default is **Keystone v2**.

> **Important**
>
> If the Keystone service is configured to use SSL, you must enter the SSL port for Keystone.

7. Select the appropriate Zone for the provider. By default, the zone is set to default.

8. In the Credentials area, under Default, provide the login credentials required for the OpenStack Infrastructure administrative user:

   - Enter the user name in the Username field.

   - Enter the password in the Password field.

   - Confirm the user password in the Confirm Password field.

   - Click **Validate** to confirm that the CloudForms Management Engine can connect to the OpenStack Infrastructure instance using the user name and password.

9. Under AMQP, provide the login credentials required for the Advanced Message Queuing Protocol messaging service:

   - Enter the administrative user name in the Username field.

   - Enter the user password in the Password field.

   - Confirm the user password in the Confirm Password field.

   - Click **Validate** to confirm CFME can connect to the messaging service.

10. Under RSA key pair, provide the user name and private key required to connect via SSH to all hosts in the provider:

    - Enter the administrative user name in the Username field.

    - Enter the private key from the machine on which OpenStack was deployed in the Private Key field.

11. Click **Add**.

> **Note**
>
> CloudForms Management Engine requires that the adminURL endpoint for all OpenStack services be on a non-private network. Accordingly, assign the adminURL endpoint an IP address of something other than **192.168.x.x**. The adminURL endpoint must be accessible to the CFME Appliance that is responsible for collecting inventory and gathering metrics from the OpenStack environment.

> **Note**
>
> For Red Hat CloudForms to be able to receive events from a Red Hat OpenStack provider, the OpenStack configuration file must be modified. Specifically, the notification_driver field must be defined.
>
> For Nova and Heat, in order to start getting notifications, manually change the configuration files as below and restart services.
>
> ```
> /etc/heat/heat.conf
> notification_driver=glance.openstack.common.notifier.rpc_notifie
> r
> notification_topics=notifications
> ```
>
> ```
> /etc/nova/nova.conf
> notification_driver=messaging
> notification_topics=notifications
> ```

1.4. VMWARE VCENTER PROVIDERS

To use a VMWare vCenter provider, add it to the appliance and authenticate its hosts.

1.4.1. Adding a VMware vCenter Provider

After initial installation and creation of a CloudForms Management Engine environment, add a VMware vCenter provider to the appliance.

1. Navigate to **Infrastructure → Providers**.

2. Click **(Configuration)**, then click **(Add a New Infrastructure Provider)**.

3. Enter the Name of the provider to add. The Name is how the device is labeled in the console.

4. Select VMware vCenter from the Type list.

5. Enter the Host Name or IP address(IPv4 or IPv6) of the provider.

> **Important**
>
> The Host Name must use a unique fully qualified domain name.

6. Select the appropriate Zone for the provider. By default, the zone is set to default.

7. In the Credentials area, under Default, provide the login credentials required for the VMware vCenter administrative user:

   ≫ Enter the user name in the Username field.

   ≫ Enter the password in the Password field.

   ≫ Confirm the password in the Confirm Password field.

   ≫ Click **Validate** to confirm CFME can connect to the VMware vCenter.

8. Click **Add**.

1.4.2. Authenticating VMware vCenter Hosts

The procedure below describes how to authenticate the VMware vCenter hosts.

1. Navigate to **Infrastructure → Providers**.

2. Click on a provider to display its summary screen.

3. On the summary screen, click Hosts in the Relationships information box to display the hosts on that provider.

4. Select the hosts to authenticate. You can select all hosts using the Check All option.

5. Click ⚙ **(Configuration)**

6. Click ✎ **(Edit Selected items)**.

7. In the Credentials area, under Default, provide the VMware ESXi login credentials:

   ≫ Enter the user name in the Username field.

   ≫ Enter the password in the Password field.

   ≫ Confirm the password in the Confirm Password field.

   ≫ Click **Validate** to confirm CFME can connect to the VMware vCenter host.

8. If editing multiple hosts, select a host from the Select Host to validate against list; provide the VMware ESXi login credentials and click **Validate**.

9. Click **Save**.

1.4.2.1. Using a Non-Administrator Account for Host Credentials

After adding a VMware vCenter infrastructure provider, you must authenticate its hosts to enable full functionality. You can use administrator credentials, or create another user assigned to a role created for Red Hat CloudForms Management Engine. See the VMware documentation for instructions on how to create a role. You need to enable the following privileges:

From the Global group, check:

≫ Cancel task

≫ Diagnostics

≫ Log Event

≫ Set custom attribute

≫ Settings

The entire set of privileges for the following groups should be checked:

≫ Alarms

≫ Datastores

≫ dvPort Group

≫ Host

≫ Network

≫ Resource

≫ Scheduled Task

≫ Tasks

≫ Virtual Machine

≫ vSphere Distributed Switch

Additionally, you must assign the new role to the following objects:

≫ **Datacenter**: At the Datacenter the CloudForms Management Engine (CFME) (formerly EVM) user/group must have at least the read-only role at the Datacenter level (Not Propagated) to be able to see the datacenter. Without this access, relationships cannot be made. Specifically, the datastores will not show up.

≫ **Cluster**: Each Cluster that the CloudForms Management Engine needs access to must have the new role assigned and propagated.

≫ **Folders**: Each Folder that CloudForms Management Engine needs access to must have the new role assigned and propagated.

≫ **Datastores**: Each Datastore that CloudForms Management Engine needs access to must have the new role assigned and propagated.

≫ **Networking**: Each vLAN or Port Group that CloudForms Management Engine needs access to must have the new role assigned and propagated.

1.5. MICROSOFT SCVMM PROVIDERS

To use a Microsoft System Center Virtual Machine Manager provider, add it to the appliance and set up the SCVMM server for authentication.

1.5.1. Adding a Microsoft System Center Virtual Machine Manager Provider

After initial installation and creation of a CloudForms Management Engine environment, add a Microsoft System Center Virtual Machine Manager provider to the appliance.

1. Navigate to **Infrastructure → Providers**.

2. Click ⚙ **(Configuration)**, then click ➕ **(Add a New Infrastructure Provider)**.

3. Enter the Name of the provider to add. The Name is how the device is labeled in the console.

4. Select Microsoft System Center VMM from the Type list.

5. Enter the Host Name or IP address(IPv4 or IPv6) of the provider.

   > **Important**
   >
   > The Host Name must use a unique fully qualified domain name.

6. Select Kerberos or Basic (SSL) from the Security Protocol list. The default security protocol is Kerberos.

7. If you select Kerberos as the security protocol, enter the Realm to which the Microsoft System Center Virtual Machine Manager belongs: for example, www.example.com.

8. Select the appropriate Zone for the provider. By default, the zone is set to default.

9. In the Credentials area, under Default, provide the login credentials required for the Microsoft System Center Virtual Machine Manager administrative user:

   » Enter the user name in the Username field.

   > **Note**
   >
   > A user name under the Kerberos security protocol must be in the format name@realm.

   » Enter the password in the Password field.

   » Confirm the password in the Confirm Password field.

   » Click **Validate** to confirm CFME can connect to the Microsoft System Center Virtual Machine Manager.

10. Click **Add**.

1.5.2. Authenticating to Microsoft SCVMM

You must enable WinRM to listen for HTTP traffic on Microsoft SCVMM servers in order for CloudForms Management Engine to establish a connection. You must also set the appropriate execution policy on the SCVMM server to allow PowerShell scripts from the appliance to run remotely.

Important

Support for Microsoft SCVMM is in Technology Preview. See Technology Preview Features Support Scope.

1. Log in to the Microsoft SCVMM server and enable WinRM for configuration.

   ```
   winrm quick config
   ```

2. Set the following options:

   ```
   winrm set winrm/config/client/auth @{Basic="true"}
   winrm set winrm/config/service/auth @{Basic="true"}
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```

3. For Windows 2012 R2 with PowerShell 4.0, use the following syntax to set these options:

   ```
   winrm set winrm/config/client/auth '@{Basic="true"}'
   winrm set winrm/config/service/auth '@{Basic="true"}'
   winrm set winrm/config/service '@{AllowUnencrypted="true"}'
   ```

4. Enable remote script execution on the SCVMM server using the Set-ExecutionPolicy cmdlet.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   For more information on SCVMM remote script execution policies, see Using the Set-ExecutionPolicy Cmdlet.

If PowerShell returns an error, search for **log_dos_error_results** in the *evm.log* and *scvmm.log* files for information.

1.6. REFRESHING PROVIDERS

Refresh a provider to find other resources related to it. Use Refresh after initial discovery to get the latest data about the provider and the virtual machines it can access. Ensure the provider has

credentials to do this. If the providers were added using Discovery, add credentials using **(Edit Selected Infrastructure Provider)**.

1. Navigate to **Infrastructure → Providers**.

2. Select the providers to refresh.

3. Click **(Configuration)**, and then **(Refresh Relationships and Power States)**.

4. Click **OK**.

1.7. TAGGING MULTIPLE PROVIDERS

Apply tags to all providers to categorize them together at the same time. Before assigning tags, create them using instructions in the *CloudForms Management Engine Settings and Operations Guide*.

1. Navigate to **Infrastructure → Providers**.

2. Check the providers to tag.

3. Click ![shield icon] (**Policy**), and then ![tag icon] (**Edit Tags**).

4. In the Tag Assignment area, select a customer tag to assign from the first list, then select a value to assign from the second list.
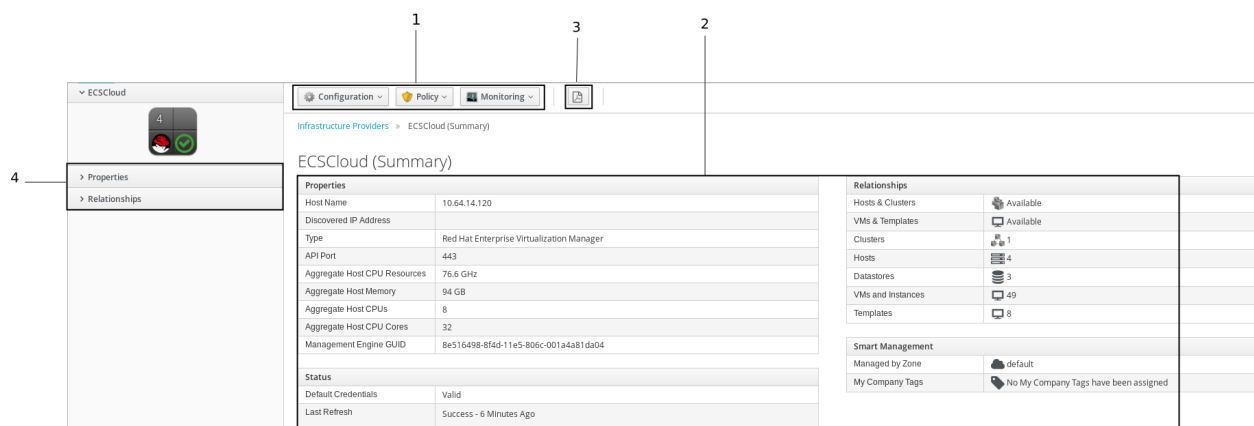
5. Select more tags as required; click **Save**.

1.8. VIEWING A PROVIDER

From a list of providers, you can review a specific provider by clicking on it. This displays various options to access provider information.

Figure 1.1. Provider Management Screen

1. Provider Taskbar: Choose between Configuration, Policy and Monitoring options for the selected provider

2. Provider Summary: Displays provider summary such as Properties, Relationships, and Smart Management

3. Provider Summary PDF: Generates provider summary in PDF format

4. Provider Accordion: Displays details about Properties and Relationships for the selected provider

1.9. REMOVING A PROVIDER

If a provider has been decommissioned or requires some troubleshooting, it might require deletion from the VMDB.

Deleting a provider removes the account information from CloudForms Management Engine console. You will no longer be able to view any associated history including chargeback reports generated for the deleted provider. Additionally, if CloudForms Management Engine is the database of record, deleting providers would become a major problem for the other systems relying on it for accurate and consistent billing information. Review all the dependencies carefully before deleting a provider.

1. Navigate to **Infrastructure → Providers**.

2. Select the check box for the provider to delete.

3. Click ![] **(Configuration)**, then ![] **(Remove Infrastructure Providers from the VMDB)**.

4. Click **OK**.

1.10. VIEWING THE PROVIDER TIMELINE

View the timeline of events for the virtual machines registered to a provider.

1. Navigate to **Infrastructure → Providers**.

2. Click a provider.

3. Click ![] **(Monitoring)**, and then ![] **(Timelines)** from the taskbar, or from the provider accordion, click **Properties → Timeline**.

4. From Options, customize the period of time to display and the types of events to see.

Options

Show	Management Events	⌄
Interval	Daily	⌄
Date	11/20/2015	
Show	7	⌄ days back
Level	Summary	⌄
Event Groups	Power Activity	⌄
	<NONE>	⌄
	<NONE>	⌄

* Dates/Times on this page are based on time zone: UTC.

» Use Show to select regular Management Events or Policy Events.

» Use the Interval dropdown to select hourly or daily data points.

» Use Date to type the date for the timeline to display.

» If you select to view a daily timeline, use Show to set how many days back to go. The maximum history is 31 days.

» The three Event Groups lists allow you to select different groups of events to display. Each has its own color.

» From the Level list, select a Summary event, or a Detail list of events. For example, the detail level of a Power On event might include the power on request, the starting event, and the actual Power On event. If you select Summary, only the Power On event displays in the timeline.

1.11. VIEWING HOSTS AND CLUSTERS

Access a tree view of the hosts and clusters for a provider from the Provider Summary.

1. Navigate to **Infrastructure → Providers**.

2. Click the provider to view the hosts and clusters.

3. Click on the Relationships accordion, then click 'Hosts & Clusters'.
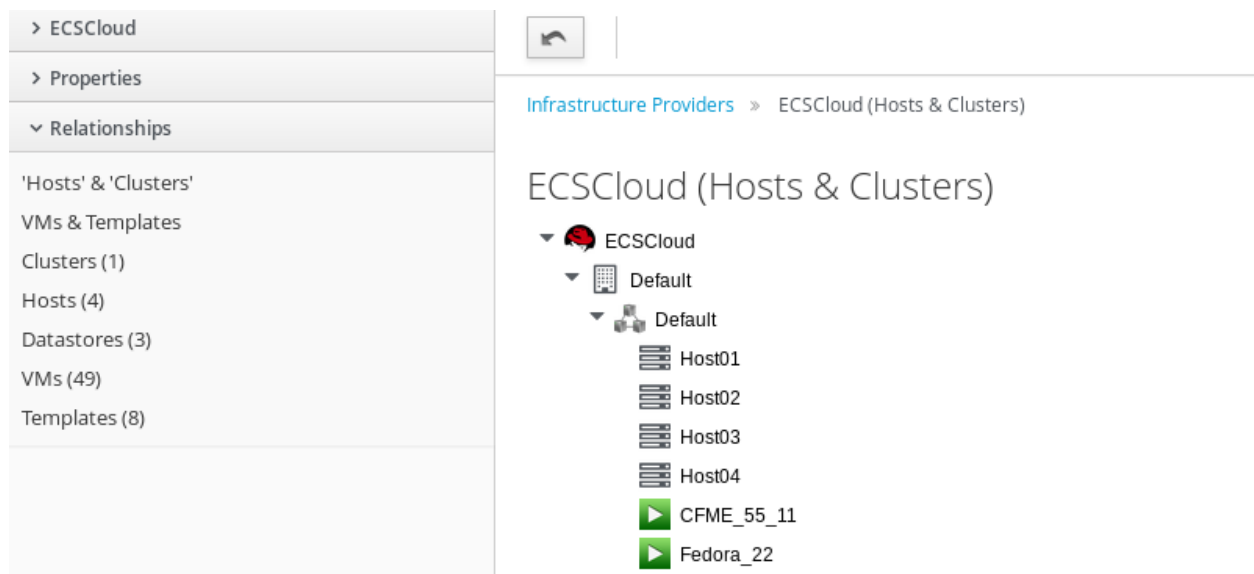
1.12. VIEWING VIRTUAL MACHINES AND TEMPLATES

Access a tree view of the virtual machines and templates for a provider from the Provider Summary.

1. Navigate to **Infrastructure → Providers**.

2. Click the provider to view the virtual machines and templates.

3. From accordion menu, click Relationships, then click VMs & Templates.

CHAPTER 2. CLOUD PROVIDERS

A cloud provider is a service that manages cloud resources. The Providers page displays all discovered or added cloud providers.

2.1. ADDING OPENSTACK PROVIDERS

CloudForms Management Engine supports operating with the OpenStack "admin" tenant. When creating an OpenStack provider in CloudForms Management Engine, select the OpenStack provider's admin user because it is the default administrator of the OpenStack admin tenant. When using the admin credentials, a user in CloudForms Management Engine provisions into the admin tenant, and sees images, networks, and instances that are associated with the admin tenant.

1. Navigate to **Clouds → Providers**.

2. Click ⚙ **(Configuration)**, then click ➕ **(Add a New Cloud Provider)**.

3. Enter a Name for the provider.

4. From the Type drop down menu select OpenStack.

5. Enter the Host Name (or IPv4 or IPv6 address) of the provider.

   > **Important**
   >
   > The Host Name must use a unique fully qualified domain name.

6. Enter the API Port of your Keystone service. The default port is **5000**.

   > **Important**
   >
   > If the Keystone service is configured to use SSL, you must enter the SSL port for Keystone.

7. Select the appropriate API Version from the list. The default is **Keystone v2**.

8. Select the appropriate Zone for the provider. By default, the zone is set to default.

9. In the Credentials area, under Default, provide the login credentials required for the Keystone user:

   > **Important**
   >
   > To enable discovery of OpenStack cloud providers, ensure that the *iptables* for the OpenStack host providing Keystone services allows port 5000 access to all hosts on the same network.

   ▸ Enter the user name in the Username field.

- Enter the user password in the Password field.

- Confirm the user password in the Confirm Password field.

- Click **Validate** to confirm CFME can connect to the OpenStack Infrastructure instance.

10. If AMQP credentials were changed during the OpenStack provider install, use the AMQP tab of the Credentials area to provide the login credentials required for the Advanced Message Queuing Protocol messaging service on your OpenStack Nova component:

   - Enter the administrative user name in the Username field.

   - Enter the user password in the Password field.

   - Confirm the user password in the Confirm Password field.

   - Click **Validate** to confirm CFME can connect to the messaging service.

11. Click **Add**.

Note

In order to collect inventory and metrics from an OpenStack environment, the CloudForms Management Engine Appliance requires that the adminURL endpoint for the OpenStack environment should be on a non-private network. Hence, the OpenStack adminURL endpoint should be assigned an IP address other than **192.168.x.x**.

Note

For Red Hat CloudForms to be able to receive events from a Red Hat OpenStack provider, the OpenStack configuration file must be modified. Specifically, the notification_driver field must be defined.

For Nova and Heat, in order to start getting notifications, manually change the configuration files as below and restart services.

```
/etc/heat/heat.conf
notification_driver=glance.openstack.common.notifier.rpc_notifie
r
notification_topics=notifications
```

```
/etc/nova/nova.conf
notification_driver=messaging
notification_topics=notifications
```

2.2. ADDING AZURE PROVIDERS

CloudForms Management Engine now supports Microsoft Azure providers. When adding an Azure provider, select a region from a list of possible regions; one provider will be created for the selected region. You can discover a set of Azure providers across all regions.

> **Note**
>
> Before Red Hat CloudForms can be authenticated to Microsoft Azure, a series of steps must be followed on Azure to create a service principal account for CloudForms; see Create Active Directory application and service principal account using the Azure portal.

After a service principal account has been created in Azure, the following three pieces of information will be available for adding an Azure provider to CloudForms:

≫ Client ID

≫ Tenant ID

≫ Client Key

Procedure: To Add an Azure Provider

1. Navigate to **Clouds → Providers**.

2. Click (Configuration), then click (Add a New Cloud Provider).

3. Enter a Name for the provider.

4. From the Type list, select Azure.

5. Select a region from the Region list.

6. Enter Tenant ID.

7. Enter Zone.

8. In the Credentials section, enter the Client ID and Client Key; click `Validate`.

9. Click `Add`.

2.3. DISCOVERING AZURE PROVIDERS

CloudForms Management Engine provides the ability to discover a set of Microsoft Azure providers across all regions.

Procedure: To Discover an Azure Provider

1. Navigate to **Clouds → Providers**.

2. Click (Configuration), then click (Discover Cloud Providers).

3. Select Azure from the Discover Type list.

4. In the Credentials section, enter the Client ID, Client Key, and Azure Tenant ID.

5. Click `Start`.

2.4. ADDING AMAZON EC2 PROVIDERS

After initial installation and creation of a CloudForms Management Engine environment, add an Amazon EC2 cloud provider by following this procedure:

Procedure: To Add Amazon EC2 Provider

1. Navigate to **Clouds → Providers**.

2. Click **(Configuration)**, then click **(Add a New Cloud Provider)**.

3. Enter a Name for the provider.

4. From the Type list select Amazon EC2.

5. Select an Amazon Region.

6. Select the appropriate Zone if you have more than one available.

7. Generate an Access Key in the Security Credentials of your Amazon AWS account. The Access Key ID acts as your User ID, and your Secret Access Key acts as your Password.

8. Click **Validate** to validate the credentials.

9. Click **Add**.

2.5. DISCOVERING AMAZON EC2 CLOUD PROVIDERS

CloudForms Management Engine provides the ability to discover cloud providers associated with a particular set of Amazon EC2 account details.

1. Navigate to **Clouds → Providers**.

2. Click **(Configuration)**, then click **(Discover Cloud Providers)**.

3. Select Amazon EC2 from the Discover Type list.

4. Enter your Amazon EC2 User ID and Password. Reenter your password in the Verify Password field.

5. Click **Start**.

2.6. ENABLING AWS CONFIG NOTIFICATIONS

Amazon's AWS Config notifies subscribers of changes in a region through its Simple Notification Service (SNS). Red Hat CloudForms subscribes to the SNS service for AWS Config deltas and converts the deltas into Red Hat CloudForms events.

1. Enable the AWS Config service in the AWS Management Console. See the AWS Config Developer Guide for more information.

2. Create a new Amazon SNS topic named **AWSConfig_topic**. CloudForms automatically connects to this topic.

3. (Optional) Configure the frequency of delta creation in the AWS Management Console.

You can assign Red Hat CloudForms policies to the AWS events listed below. The appliance performs a provider refresh on all these events except for AWS_EC2_Instance_UPDATE. See the Control Guide for more information on working with CloudForms policies.

Event	Policies	Refresh
AWS_EC2_Instance_CREATE	src_vm vm_create	ems
AWS_EC2_Instance_UPDATE	N/A	ems
AWS_EC2_Instance_running	src_vm vm_start	ems
AWS_EC2_Instance_stopped	src_vm vm_power_off	ems
AWS_EC2_Instance_shutting-down	src_vm vm_power_off	ems

2.7. REFRESHING CLOUD PROVIDERS

Refresh a cloud provider to find other resources related to it. Ensure the chosen cloud providers have the correct credentials before refreshing.

1. Navigate to **Clouds → Providers**.

2. Select the checkboxes for the cloud providers to refresh.

3. Click ⚙ `(Configuration)`, and then ↻ `(Refresh Relationships and Power States)`.

4. Click **OK**.

2.8. TAGGING CLOUD PROVIDERS

Apply tags to all cloud providers to categorize them together at the same time. Before assigning tags, create them using instructions in the *CloudForms Management Engine Settings and Operations Guide*.

Procedure: To Tag Cloud Providers

1. Navigate to **Clouds → Providers**.

2. Select the checkboxes for the Cloud Providers to tag.

3. Click ![shield] **(Policy)**, and then ![tag] **(Edit Tags)**.

4. Select a customer tag to assign from the first list.

5. Select a value to assign from the second list.

6. Click **Save**.

2.9. REMOVING CLOUD PROVIDERS

A cloud provider might require removal from the VMDB if it is no longer in use.

1. Navigate to **Clouds → Providers**.

2. Check the cloud providers to remove.

3. Click ![gear] **(Configuration)**, and then ![trash] **(Remove Cloud Providers from the VMDB)**.

4. Click **OK**.

2.10. EDITING A CLOUD PROVIDER

Edit information about a provider such as the name, IP address, and login credentials.

> **Note**
>
> The Type value is unchangeable. To use a different cloud provider, create a new one.

1. Navigate to **Clouds → Providers**.

2. Click the cloud provider to edit.

3. Click ![gear] **(Configuration)**, and then ![pencil] **(Edit Selected Cloud Provider)**.

4. Edit the Basic Information. This varies depending on the Type of provider.

5. Fill out the Credentials by typing in a Username, Password, and a verification of this password (Confirm Password).

  » If selecting Amazon EC2, generate an Access Key in the Security Credentials of your
    Amazon AWS account. The Access Key ID acts as your User ID, and your Secret
    Access Key acts as your Password.

  » If selecting OpenStack, use the Keystone User ID and Password for your login
    credentials.

6. If editing an OpenStack provider, use the AMQP subtab to provide credentials required for
   the Advanced Message Queuing Protocol service on your OpenStack Nova component.

7. Click **Validate** and wait for notification of successful validation.

8. Click **Save**.

2.11. VIEWING A CLOUD PROVIDER'S TIMELINE

View the timeline of events for instances registered to a cloud provider.

1. Navigate to **Clouds** → **Providers**.

2. Click the desired cloud provider for viewing the timeline.

3. Click **(Monitoring)**, and then **(Timelines)**.

4. From Options, customize the period of time to display and the types of events to see.

   » Use Show to select regular Management Events or Policy Events.

   » Use the Type list to select hourly or daily data points.

   » Use Date to type the date for the timeline to display.

   » If you select to view a daily timeline, use Show to set how many days back to go. The
     maximum history is 31 days.

   » The three Event Groups list allow you to select different groups of events to display.
     Each has its own color.

   » From the Level list, select a Summary event, or a Detail list of events.

CHAPTER 3. CONTAINERS PROVIDERS

A containers provider is a service that manages container resources.

The Containers area in the top menu bar has options to add and manage containers providers. The Containers area includes the Providers page, which displays all discovered or added containers providers.

The supported containers provider types that you can add in CloudForms Management Engine are:

- **OpenShift Enterprise**. For information on adding this provider type, see Section 3.3, "Adding an OpenShift Provider".

- **Atomic Enterprise Platform**. For information on adding this provider type, see Section 3.4, "Adding an Atomic Enterprise Platform Provider".

To successfully add an OpenShift or Atomic Enterprise Platform provider, you must first configure a service account in a provider's cluster. For more information, see Section 3.1, "Configuring Service Accounts".

3.1. CONFIGURING SERVICE ACCOUNTS

To add an OpenShift or Atomic Enterprise Platform provider, you must create, in a provider's cluster, a specific `management` service account with the proper role, permissions, and authentication token.

For more information on these topics, see the relevant documentation:

- Kubernetes Service Accounts

- Kubernetes Authentication

- OpenShift Service Accounts

To add a `management` service account in an OpenShift cluster, follow these steps:

1. Open a terminal and run the following commands:

   ```
   $ oadm new-project management-infra --description="Management
   Infrastructure"
   ```

   ```
   $ oc create -n management-infra -f - <<EOF
   apiVersion: v1
   kind: ServiceAccount
   metadata:
     name: management-admin
   EOF
   ```

   ```
   $ oc create -f - <<EOF
   apiVersion: v1
   kind: ClusterRole
   metadata:
     name: management-infra-admin
   rules:
   - resources:
   ```

```
  - pods/proxy
  verbs:
  - '*'
EOF
```

```
$ oadm policy add-role-to-user -n management-infra admin -z
management-admin
```

```
$ oadm policy add-role-to-user -n management-infra management-
infra-admin -z management-admin
```

```
$ oadm policy add-cluster-role-to-user cluster-reader
system:serviceaccount:management-infra:management-admin
```

```
$ oadm policy add-scc-to-user privileged
system:serviceaccount:management-infra:management-admin
```

> **Note**
>
> At the moment, the **management-infra-admin** role is needed to address the
> OpenShift issue #5973.

2. To obtain the **management** service account token name, run:

```
oc get -n management-infra sa/management-admin --
template='{{range .secrets}}{{printf "%s\n" .name}}{{end}}'
management-admin-token-32f97
management-admin-dockercfg-fvkso
```

3. To retrieve the token, run:

```
$ oc get -n management-infra secrets management-admin-token-32f97
--template='{{.data.token}}' | base64 -d
eyJhbGciOiJSUzI1NiIsInR5cC...
```

Replace **management-admin-token-32f97** with the name of your token.

Now it is possible to use the token to add a containers provider in CloudForms Management Engine.

3.2. CONFIGURING OPENSHIFT METRICS

To collect the **nodes**, **pods**, and **containers** metrics, it is required to run the OpenShift Metrics
services inside your cluster. For more information, see the OpenShift Enterprise Metrics
Documentation.

> **Note**
>
> Use the OpenShift master public host name as the **HAWKULAR_METRICS_HOSTNAME**, at the moment a limitation in CloudForms Management Engine is assuming that the provider **Host Name** is used also to collect the metrics.

Once Hawkular Metrics and Heapster have been successfully deployed by OpenShift Metrics, it is possible to create a router for CloudForms Management Engine to access the metrics data:

```
oadm router management-metrics \
  --credentials=/etc/origin/master/openshift-router.kubeconfig \
  --service-account=router --ports='443:5000' \
  --selector='kubernetes.io/hostname=<INSERT MASTER HOSTNAME HERE>'
  --stats-port=1937 \
  --host-network=false
```

This router must, at the moment, be run on the master nodes to expose the metrics on the port **5000** to CloudForms Management Engine, hence the need for a **selector** on the **kubernetes.io/hostname** of the master node.

As long as the router or routers are accessible from the same public host name of the master, it is possible to use different selectors and scale the number of replicas in order to achieve high availability.

3.3. ADDING AN OPENSHIFT PROVIDER

After initial installation and creation of a CloudForms Management Engine environment and configuration of an OpenShift cluster service account, add an OpenShift provider by following the procedure below.

For information on how to configure an OpenShift cluster service account, see Section 3.1, "Configuring Service Accounts".

Procedure: To Add an OpenShift Provider

1. Navigate to **Containers → Providers**.

2. Click ⚙ **Configuration**, then click ➕ **Add a New Containers Provider**.

3. Enter a Name for the provider.

4. From the Type drop-down menu select OpenShift.

5. Enter the Hostname or IP address of the provider.

   > **Important**
   >
   > The Hostname must use a unique fully qualified domain name.

6. Enter the Port of the provider. The default port is **8443**.

7. Select the appropriate Zone for the provider. By default, the zone is set to default.

8. Under Credentials, enter the token in the Token field.

   * Click **Validate** to confirm that the CloudForms Management Engine can connect to the OpenShift provider using the provided token.

9. Click **Add**.

3.4. ADDING AN ATOMIC ENTERPRISE PLATFORM PROVIDER

After initial installation and creation of a CloudForms Management Engine environment and configuration of an Atomic Enterprise Platform cluster service account, add an Atomic Enterprise Platform provider by following the procedure below.

For information on how to configure an Atomic Enterprise Platform cluster service account, see Section 3.1, "Configuring Service Accounts".

Procedure: To Add an Atomic Enterprise Platform Provider

1. Navigate to **Containers → Providers**.

2. Click **Configuration**, then click **Add a New Containers Provider**.

3. Enter a Name for the provider.

4. From the Type drop-down menu select Atomic Enterprise.

5. Enter the Hostname or IP address of the provider.

   Important

   The Hostname must use a unique fully qualified domain name.

6. Enter the Port of the provider. The default port is **8443**.

7. Select the appropriate Zone for the provider. By default, the zone is set to default.

8. Under Credentials, enter the token in the Token field.

   * Click **Validate** to confirm that the CloudForms Management Engine can connect to the OpenShift provider using the provided token.

9. Click **Add**.

3.5. TAGGING CONTAINERS PROVIDERS

Apply tags to all containers providers to categorize them together at the same time. Before assigning tags, create them using instructions in the *Red Hat CloudForms 4.0 General Configuration Guide*, available from https://access.redhat.com/documentation/en/red-hat-cloudforms/.

Procedure: To Tag Containers Providers

1. Navigate to **Containers → Providers**.

2. Select the checkboxes for the containers providers to tag.

3. Click **Policy**, and then `Edit Tags`.

4. Select a customer tag to assign from the drop-down menu.

5. Select a value to assign.

6. Click **Save**.

3.6. REMOVING CONTAINERS PROVIDERS

A containers provider might require removal from the VMDB if it is no longer in use.

Procedure: To Remove Containers Providers

1. Navigate to **Containers → Providers**.

2. Select the checkboxes for the containers providers to remove.

3. Click `Configuration`, and then `Remove Containers Providers from the VMDB`.

4. Click **OK**.

3.7. EDITING A CONTAINERS PROVIDER

Edit information about a provider such as the name, hostname or IP address, and credentials.

Procedure: To Edit a Containers Provider

1. Navigate to **Containers → Providers**.

2. Click the containers provider to edit.

3. Click `Configuration`, and then `Edit Selected Containers Provider`.

4. Edit the Basic Information. This varies depending on the Type of provider.

> **Note**
>
> The Type value is unchangeable. To use a different containers provider, create a new one.

5. Edit the Credentials by typing in a new Token.

6. Click Validate and wait for notification of successful validation.

7. Click **Save**.

3.8. VIEWING A CONTAINERS PROVIDER'S TIMELINE

View the timeline of events for instances registered to a containers provider.

Procedure: To View a Containers Provider's Timeline

1. Navigate to **Containers → Providers**.

2. Click the desired containers provider for viewing the timeline.

3. Click `Monitoring`, and then `Timelines`.

4. From Options, customize the period of time to display and the types of events to see.

   » Use Show to select regular Management Events or Policy Events.

   » Use the Interval dropdown to select hourly or daily data points.

   » Use Date to type the date for the timeline to display.

   » If you select to view a daily timeline, use Show to set how many days back to go. The maximum history is 31 days.

   » From the Level dropdown, select a Summary event, or a Detail list of events.

   » The three Event Groups dropdowns allow you to select different groups of events to display. Each has its own color.

To see more detail on an item in the timeline, click on it. A balloon appears with a link to the resource.

CHAPTER 4. MANAGING CONTAINERS

Red Hat CloudForms 4.0 allows for container management along with image and flavor management for instances. The orchestration system can be OpenShift or Atomic Enterprise Platform, and it can work with both RHEV and VMware providers.

The Containers area in the top menu bar has options to manage containers, containers providers, images, nodes, registries, podes, and other components.

4.1. CORE CONCEPTS

The following is a list of some of the core concepts and objects you will encounter when using CloudForms Management Engine with OpenShift or Atomic Enterprise Platform. Many of these objects come from Kubernetes, which is extended by OpenShift to provide a more feature-rich development life cycle platform.

➤ **Node** is a machine that containers run on. For more information, see OpenShift Enterprise 3.1 Architecture Information

➤ **Pod** is a group of containers. For more information, see OpenShift Enterprise 3.1 Architecture Information.

➤ **Replication controller** ensures that there is always a certain number of pods available. For more information, see OpenShift Enterprise 3.1 Architecture Information.

➤ **Service** is a base load balancer that provides traffic to pods. For more information, see OpenShift Enterprise 3.1 Architecture Information.

➤ **Namespace** is an ability to partition resources created by users into logical groups. For more information, see OpenShift Enterprise 3.1 Architecture Information.

4.2. INSIGHT AND CONTROL

CloudForms Management Engine can connect to OpenShift and Atomic Enterprise Platform containers providers and supports managing them similarly to how infrastructure and cloud providers are managed. This allows you to gain control over different aspects of your environment and answer questions such as:

➤ How many containers exist in my environment?

➤ Does a specific node have enough resources?

➤ How many distinct images are used?

➤ Which image registries are used?

When CloudForms Management Engine connects to a containers provider, it collects information on different areas of the provider environment:

➤ Entities such as pods, nodes, or services.

➤ Basic relationships between the entities, for example: Which services are serving which pods?

➤ Advanced insight into relationships, for example: Which two different containers are using the same image?

➤ Additional information, such as services, events, projects, namespaces, routes (OpenShift only), and metrics.

4.2.1. Cross-Providers Insight

Cross-providers insight is a feature that connects all layers of infrastructure, cloud, and containers known to CloudForms Management Engine and collects data for analysis.

It supports cross-linking with the following environments:

➤ OpenStack

➤ oVirt or RHEV

➤ VMware vCenter

The collected data includes information on traffic, storage, and so on.

4.2.2. Working with the Containers Overview Page

The information on all containers providers and entities known to CloudForms Management Engine is summarized on the Containers Overview page. The Overview page provides links to other summary pages which contain further information on the containers providers and entities.
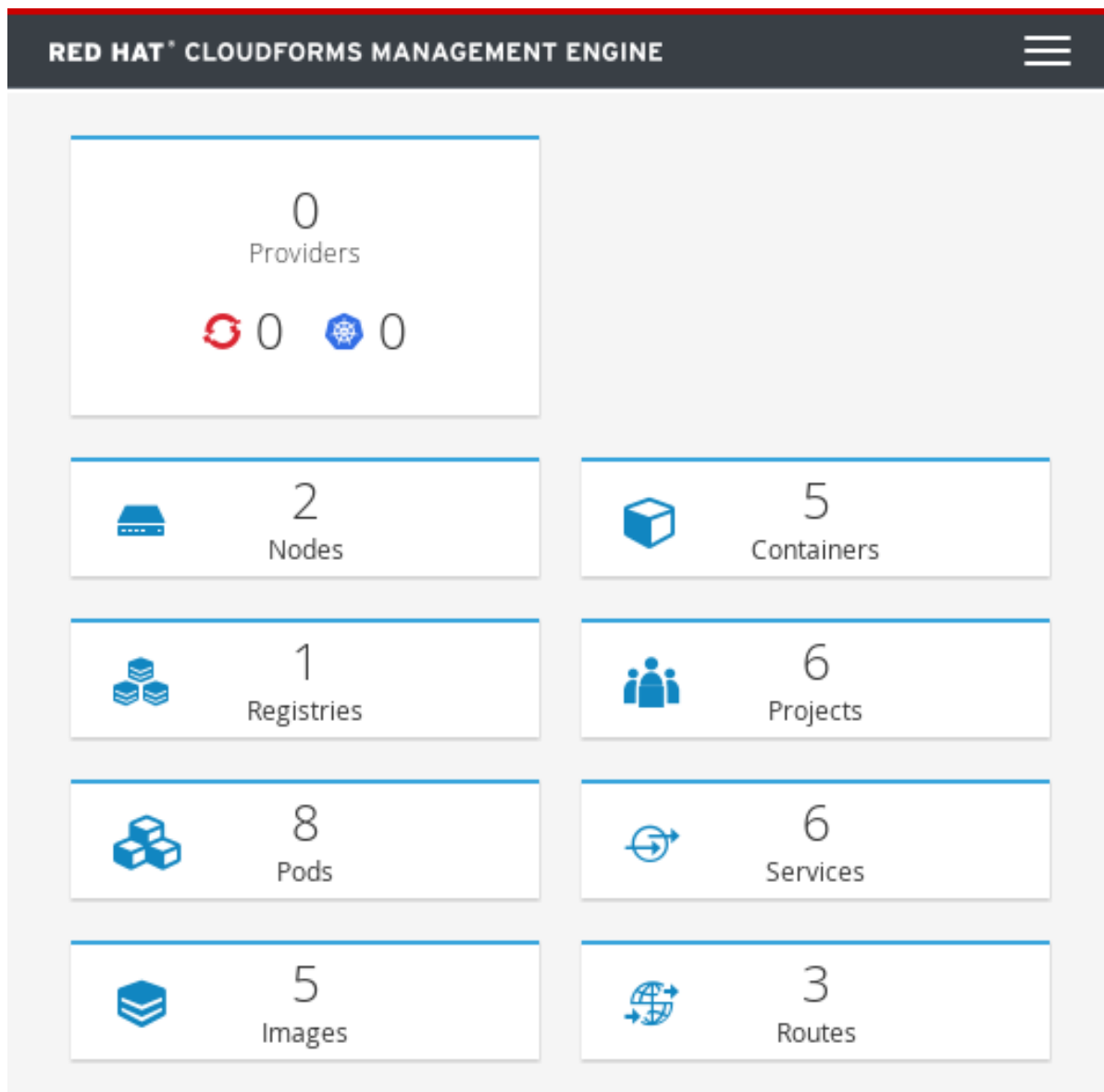
Working with the Containers Overview Page

1. Navigate to **Containers → Overview**.

2. Click the desired containers provider or entity for viewing the summary with further information.

4.2.3. Viewing a Containers Provider Summary

A Containers Provider summary page allows you to view information on different aspects of a containers provider, for example:

» Status of the provider and its components.

» Relationships between different entities of the containers provider. These relationships are summarized in the Relationships box on the right-hand side of the summary page.

> ❯ Additional information on the number of aggregate node CPU cores or aggregate node memory.

Viewing a Containers Provider Summary

1. Navigate to **Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

4.2.4. Viewing a Container Nodes Summary

A Container Node summary page allows you to view information on different aspects of a container node, for example:

> ❯ How many entities are on a node?

> ❯ What is the capacity and utilization?

> ❯ What are the versions of the underlying operating system and software?

Viewing a Container Nodes Summary

1. Navigate to **Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the Relationships box on the right-hand side of the summary page, click Nodes.

4. Click the desired container node for viewing.

4.2.5. Viewing a Containers Summary

A Containers summary page allows you to view information on different aspects of a container, for example:

» Which node is the container running on?

» Which part of a pod is the container?

» What is the container ID?

» What is the container image name?

Viewing a Containers Summary

1. Navigate to **Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the Relationships box on the right-hand side of the summary page, click Containers.

4. Click the desired container for viewing.

4.2.6. Viewing a Container Images Summary

A Container Images summary page allows you to view information on different aspects of a container image, for example:

» Which containers are using the image?

» Which image registry is the image coming from? Is it a certified registry?

Viewing a Container Images Summary

1. Navigate to **Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the Relationships box on the right-hand side of the summary page, click Images.

4. Click the desired image for viewing.

4.2.7. Viewing an Image Registries Summary

An Image Registries summary page allows you to view information on different aspects of an image registry, for example:

» How many images are coming from the registry? What are the images?

» Which containers are using images from the registry?

Viewing an Image Registries Summary

1. Navigate to **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the Relationships box on the right-hand side of the summary page, click Image Registries.

4. Click the desired image registry for viewing.

4.2.8. Viewing a Pods Summary

A Pods summary page allows you to view information on different aspects of a pod, for example:

➤ Which containers are part of the pod?

➤ Which services work with the pod?

➤ Which services does the pod run on?

➤ Is the pod controlled by a replicator?

Viewing a Pods Summary

1. Navigate to **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the Relationships box on the right-hand side of the summary page, click Pods.

4. Click the desired pod for viewing.

4.2.9. Viewing a Replicators Summary

A Replicators summary page allows you to view information on different aspects of a replicator, for example:

➤ What is the number of requested pods?

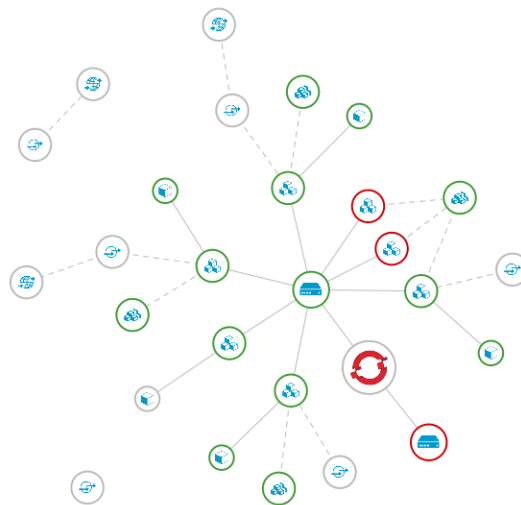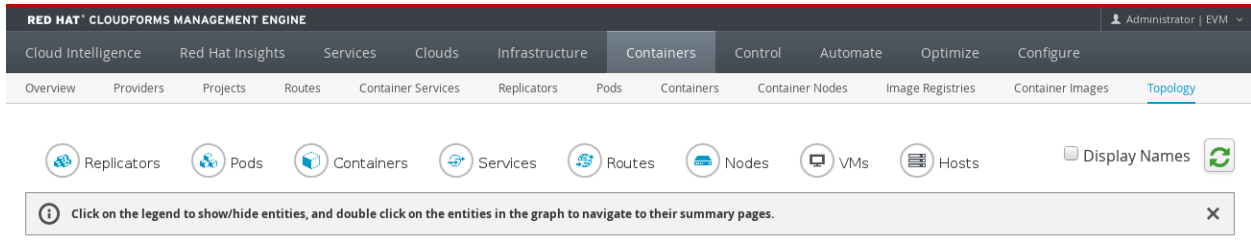➤ What is the number of current pods?

Viewing a Replicators Summary

1. Navigate to **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the Relationships box on the right-hand side of the summary page, click Replicators.

4. Click the desired replicator for viewing.

4.2.10. Using the Topology Widget

The Topology widget is an interactive topology graph, showing the relationships between the different entities of the containers providers that CloudForms Management Engine has access to.

❧ The topology graph includes pods, containers, services, nodes, virtual machines, and hosts within the overall containers provider environment.

❧ Selecting any individual graph node will display a summary of details for the individual node.

❧ It is possible to drag elements to reposition the graph and to zoom in for details on a specific subset of items.

Viewing the Topology Widget

1. Navigate to **Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. On the provider summary page, click Topology in the Overview box on the right-hand side of the page.

4.2.11. Running a SmartState Analysis

Perform a SmartState Analysis of a container image to inspect the packages included in an image and get information on all new or updated packages.

Running a SmartState Analysis

1. Navigate to **Containers → Container Images**.

2. Check the container image to analyze. You can check multiple images.

3. Click **Configuration**, and then **Perform SmartState Analysis**.

The container image is scanned. The process will copy over any required files and install any required packages for the image. After reloading the image page, all new or updated packages are listed.

CHAPTER 5. DATASTORES

A storage location is considered a device where digital information resides and is connected to a resource. CloudForms Management Engine detects, analyzes, and collects capacity and utilization data for both VMFS and NFS datastores. Datastores connected to a provider are automatically created on discovery. On creation of a repository, a datastore is automatically created.
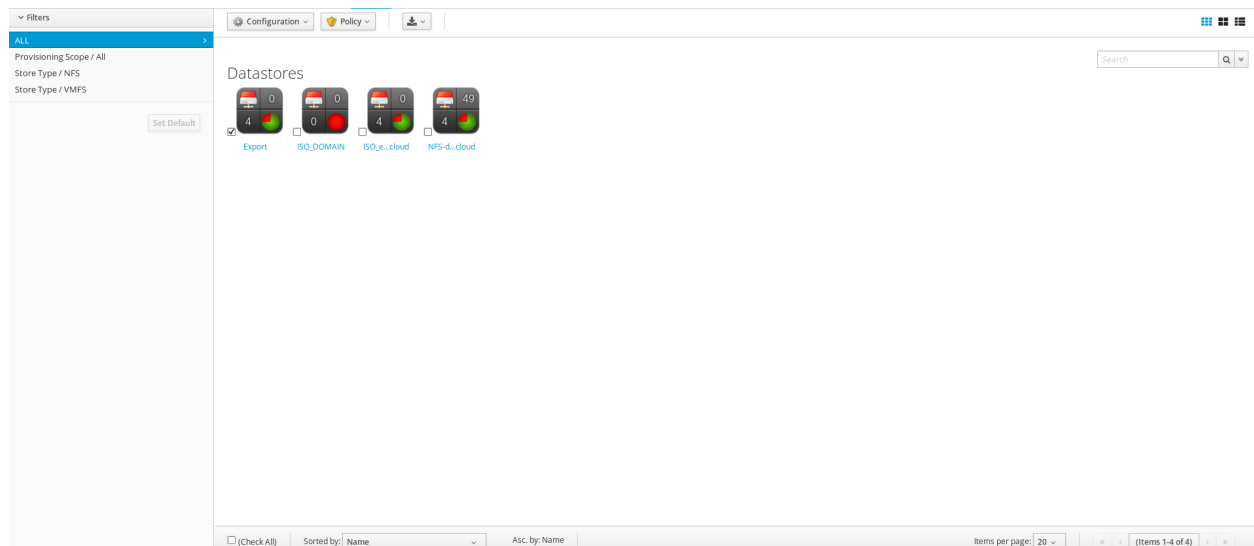
After detecting datastores, you might want to examine them more closely to see virtual machines, hosts, and available space.

1. Top left quadrant: File system type

2. Bottom left quadrant: Number of hosts

3. Top right quadrant: Number of virtual machines

4. Bottom right quadrant: Available space

5.1. PERFORMING SMARTSTATE ANALYSIS ON DATASTORES

Analyze a datastore to collect information on the types of files on a datastore, and to see the number of managed/registered, managed/unregistered, and unmanaged virtual machines. To perform a SmartState analysis, the datastore is accessible from a running host and valid security credentials are supplied for that host.

> **Note**
>
> Be aware that executing a SmartState Analysis on a datastore from the console takes a while to return data on the content. If Capacity and Utilization roles are enabled, CloudForms Management Engine performs the analysis automatically on a scheduled basis approximately every 24 hours.

1. Navigate to **Infrastructure → Datastores**.

2. Select the datastores to analyze.

3. Click ⚙ **(Configuration)**, and then 🔍 **(Perform SmartState Analysis)**.

4. Click **OK**.

5.2. VIEWING A DATASTORE

You can click on a specific Datastore to view its details. The screen provides you with a Datastore Taskbar, Virtual Thumbnail, Accordion, and Summary.

Figure 5.1. Datastore Management Screen
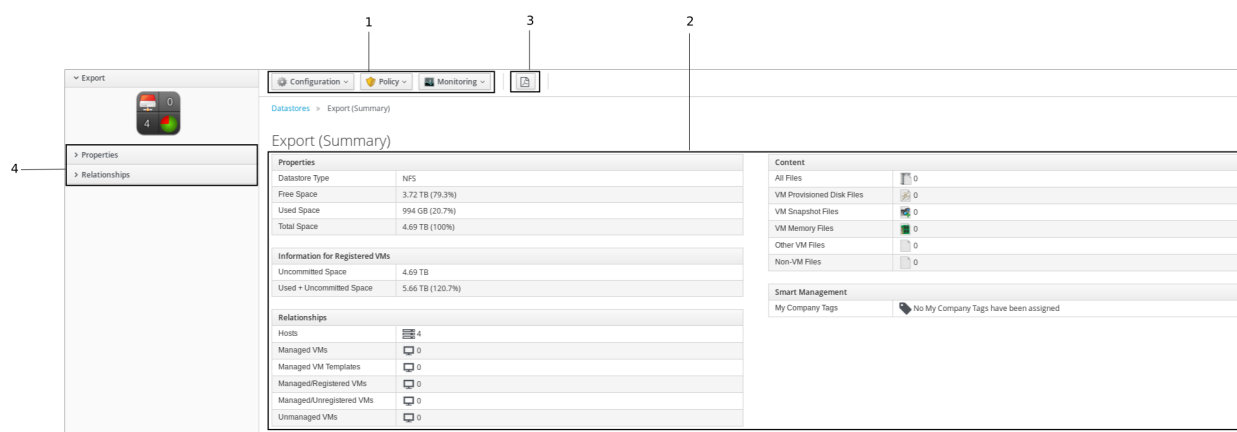
1. Datastore Taskbar: Choose between Configuration, Policy and Monitoring options for the selected Datastore

2. Datastore Summary: See summary such as datastore properties, storage, VM information.

3. Datastore PDF: Generates datastore summary in PDF format.

4. Datastore Accordion: See details about Properties, Relationships, Storage Relationships and Content for the chosen datastore.

> **Note**
>
> To view Content section details, run a SmartState Analysis on the datastore. For information on how to perform SmartState Analysis, see Performing SmartState Analysis on Datastores.

5.3. TAGGING A DATASTORE

Use tags to categorize a datastore. Before assigning tags, create them with instructions in the *CloudForms Management Engine Settings and Operations Guide*.

1. Navigate to **Infrastructure → Datastores**.

2. Click the datastore to tag.

3. Click **(Policy)**, and then **(Edit Tags)**.

4. Select a customer tag from the first list, and then a value for the tag from the second list.

5. Select more tags or click **Save** to save your changes.

5.4. VIEWING CAPACITY AND UTILIZATION CHARTS FOR A DATASTORE

You can view capacity and utilization data for a datastore.

> **Note**
>
> CloudForms Management Engine requires network visibility to your provider assigned the server role of Capacity & Utilization Collector to enable this feature.

1. Navigate to **Infrastructure → Datastores**, then click the Datastore that you want to view Capacity and Utilization data for.

2. Click **(Monitoring)**, and then (**Utilization**) or from the Datastore Accordion, click **Properties → Capacity & Utilization**.

3. From Interval, select to view hourly or daily data points and the dates to view data. Use VM Types to Include to include only managed/registered, managed/unregistered, or unmanaged virtual machines. The following definitions will be helpful.

   ➢ *Managed/Registered VM* - A virtual machine connected to a host and exists in the VMDB. Also, a template connected to a management system and exists in the VMDB.

   > **Note**
   >
   > Templates cannot be connected to a Host.

⫸ *Managed/Unregistered VM* - A virtual machine or template that resides on a repository or is no longer connected to a management system or host and exists in the VMDB. A virtual machine previously considered registered might become unregistered if the virtual machine is removed from management system inventory.

⫸ *Not Managed* - Files discovered on a datastore that do not have a virtual machine associated with them in the VMDB. These files might be registered to a management system that CloudForms Management Engine does not have configuration information. Possible causes might be the management system has not been discovered or the management system has been discovered but no security credentials are provided.

Use Time Profiles to select a time range for the data.

Note

Daily charts only include full days of data. If a day does not include all the 24 data points for a day, the data does not show for that day.

5.5. REMOVING A DATASTORE

If a datastore no longer contains any files associated with the virtual environment, remove it from the VMDB. This button is enabled only if a datastore is completely empty.

1. Navigate to **Infrastructure → Datastores**.

2. Click on the Datastore to remove.

3. Click ⚙ **(Configuration)**, and then 🗑 **(Remove Datastore from the VMDB)**.

4. Click **OK**.