CloudForms 3.1
Management Engine 5.3
Settings and Operations Guide

A guide to configuring and tuning CloudForms Management Engine

Red Hat CloudForms Documentation Team

CloudForms 3.1 Management Engine 5.3 Settings and Operations Guide

A guide to configuring and tuning CloudForms Management Engine

Red Hat CloudForms Documentation Team

Legal Notice

Abstract

This guide provides instructions on configuring CloudForms Management Engine, including appliance settings, access control, web console appearance, registration, and updates. Information and procedures in this book are relevant to CloudForms Management Engine administrators.

Table of Contents

Chapter 1. Introduction to Red Hat CloudForms

Red Hat CloudForms Management Engine delivers the insight, control, and automation enterprises need to address the challenges of managing virtual environments. This technology enables enterprises with existing virtual infrastructures to improve visibility and control, and those starting virtualization deployments to build and operate a well-managed virtual infrastructure.

Red Hat CloudForms 3.1 is comprised of a single component, the CloudForms Management Engine. It has the following feature sets:

- Insight: Discovery, Monitoring, Utilization, Performance, Reporting, Analytics, Chargeback, and Trending.
- Control: Security, Compliance, Alerting, and Policy-Based Resource, and Configuration Enforcement.
- Automate: IT Process, Task and Event, Provisioning, and Workload Management and Orchestration.
- Integrate: Systems Management, Tools and Processes, Event Consoles, Configuration Management Database (CMDB), Role-based Administration (RBA), and Web Services.

1.1. Architecture

The diagram below describes the capabilities of Red Hat CloudForms Management Engine. Its features are designed to work together to provide robust management and maintenance of your virtual infrastructure.

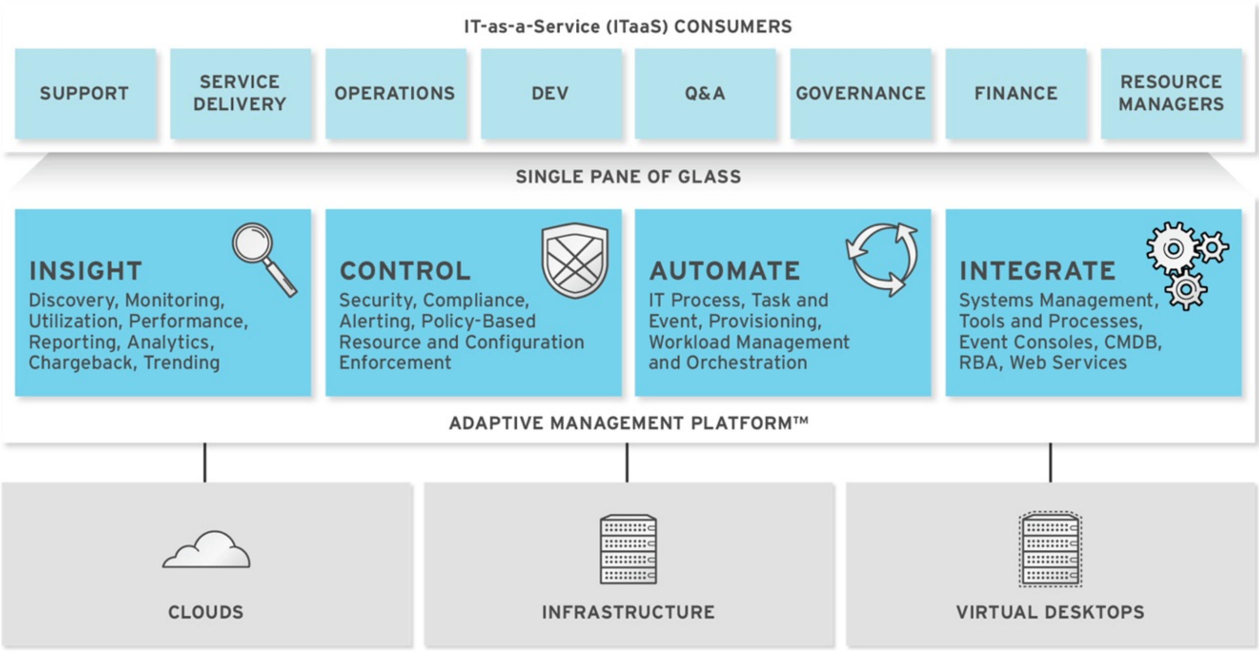

IT-as-a-Service (ITaaS) CONSUMERS
SUPPORT
SERVICE DELIVERY
OPERATIONS
DEV
Q&A
GOVERNANCE
FINANCE
RESOURCE MANAGERS
SINGLE PANE OF GLASS
INSIGHT
Discovery, Monitoring, Utilization, Performance, Reporting, Analytics, Chargeback, Trending
CONTROL
Security, Compliance, Alerting, Policy-Based Resource and Configuration Enforcement
AUTOMATE
IT Process, Task and Event, Provisioning, Workload Management and Orchestration
INTEGRATE
Systems Management, Tools and Processes, Event Consoles, CMDB, RBA, Web Services
ADAPTIVE MANAGEMENT PLATFORM™
CLOUDS
INFRASTRUCTURE
VIRTUAL DESKTOPS

Figure 1.1. Features

The architecture comprises the following components:

- The CloudForms Management Engine Appliance (Appliance) which is supplied as a secure, high-performance, preconfigured virtual machine. It provides support for Secure Socket Layer (SSL) communications.

- The CloudForms Management Engine Server (Server) resides on the Appliance. It is the software layer that communicates between the SmartProxy and the Virtual Management Database. It includes support for Secure Socket Layer (SSL) communications.

- The Virtual Management Database (VMDB) resides either on the Appliance or another computer accessible to the Appliance. It is the definitive source of intelligence collected about your Virtual Infrastructure. It also holds status information regarding Appliance tasks.

- The CloudForms Management Engine Console (Console) is the Web interface used to view and control the Server and Appliance. It is consumed through Web 2.0 mash-ups and web services (WS Management) interfaces.

- The SmartProxy can reside on the Appliance or on an ESX Server. If not embedded in the Server, the SmartProxy can be deployed from the Appliance. Each storage location must have a SmartProxy with visibility to it. The SmartProxy acts on behalf of the Appliance communicating with it over HTTPS (SSL) on standard port 443.

1.2. Requirements

To use CloudForms Management Engine, the following requirements must be met:

- One of the following Web Browsers:

  - Mozilla Firefox for versions supported under Mozilla's Extended Support Release (ESR) [1]

  - Internet Explorer 8 or higher

  - Google Chrome for Business

- A monitor with minimum resolution of 1280x1024.

- Adobe Flash Player 9 or above. At the time of publication, you can access it at http://www.adobe.com/products/flashplayer/.

- The CloudForms Management Engine Appliance must already be installed and activated in your enterprise environment.

- The SmartProxy must have visibility to the virtual machines and cloud instances that you want to control.

- The resources that you want to control must have a SmartProxy associated with them.

Regions and Zones

Use **regions** for centralizing data which is collected from public and private virtualization environments. A region is ultimately represented as a single database for the VMDB. Regions are particularly useful when multiple geographical locations need to be managed as they enable all the data collection to happen at each particular location and avoids data collection traffic across slow links between networks.

When multiple regions are being used, each with their own unique ID, a master region can be created to centralize the data of all the children regions into a single master database. To do this, configure each child region to replicate its data to the master region database (Red Hat recommends use of region 99). This parent and child region is a one-to-many relationship.

Regions can contain multiple zones, which in turn contain appliances. Zones are used for further segregating network traffic along with enabling failover configurations. Each appliance has the capability to be configured for a number of specialized server roles. These roles are limited to the zone containing the appliance they run on. If multiple appliances in a zone are configured with duplicate server roles, CFME determines whether the roles use a failover configuration or dependent on the role, as yet another resource for executing its specialized tasks.

Note

- Replicating a parent region to a higher-level parent is not supported.
- Parent region can be configured after the child regions are online.

Important

Due to browser limitations, Red Hat supports logging in to only one tab for each multi-tabbed browser. Console settings are saved for the active tab only. For the same reason, CloudForms Management Engine does not guarantee that the browser's **Back** button will produce the desired results. CloudForms Management Engine recommends using the breadcrumbs provided in the Console.

1.3. Terminology

The following terms are used throughout this document. Review them before proceeding.

Account Role

A designation assigned to a user allowing or restricting a user to parts and functions of the CloudForms Management Engine console.

Action

An execution that is performed after a condition is evaluated.

Alert

CloudForms Management Engine alerts notify administrators and monitoring systems of critical configuration changes and threshold limits in the virtual environment. The notification can take the form of either an email or an SNMP trap.

Analysis Profile

A customized scan of hosts, virtual machines, or instances. You can collect information from categories, files, event logs, and registry entries.

Cloud

A pool of on-demand and highly available computing resources. The usage of these resources are scaled depending on the user requirements and metered for cost.

CloudForms Management Engine Appliance

A virtual machine on which the virtual management database (VMDB) and CloudForms Management Engine server reside.

CloudForms Management Engine Console

A web-based interface into the CloudForms Management Engine Appliance.

CloudForms Management Engine Role

A designation assigned to a CloudForms Management Engine server that defines what a CloudForms Management Engine server can do.

CloudForms Management Engine Server

The application that runs on the CloudForms Management Engine Appliance and communicates with the SmartProxy and the VMDB.

Cluster

Hosts that are grouped together to provide high availability and load balancing.

Condition

A test of criteria triggered by an event.

Discovery

Process run by the CloudForms Management Engine server which finds virtual machine and cloud providers.

Drift

The comparison of a virtual machine, instance, host, cluster to itself at different points in time.

Event

A trigger to check a condition.

Event Monitor

Software on the CloudForms Management Engine Appliance which monitors external providers for events and sends them to the CloudForms Management Engine server.

Host

A computer on which virtual machine monitor software is loaded.

Instance/Cloud Instance

A on-demand virtual machine based upon a predefined image and uses a scalable set of hardware resources such as CPU, memory, networking interfaces.

Managed/Registered VM

A virtual machine that is connected to a host and exists in the VMDB. Also, a template that is connected to a provider and exists in the VMDB. Note that 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 provider or host and exists in the VMDB. A virtual machine that was previously considered registered may become unregistered if the virtual machine was removed from provider inventory.

Provider

A computer on which software is loaded which manages multiple virtual machines that reside on multiple hosts.

Policy

A combination of an event, a condition, and an action used to manage a virtual machine.

Policy Profile

A set of policies.

Refresh

A process run by the CloudForms Management Engine server which checks for relationships of the provider or host to other resources, such as storage locations, repositories, virtual machines, or instances. It also checks the power states of those resources.

Regions

Regions are used to create a central database for reporting and charting. Regions are used primarily to consolidate multiple VMDBs into one master VMDB for reporting.

Resource

A host, provider, instance, virtual machine, repository, or datastore.

Resource Pool

A group of virtual machines across which CPU and memory resources are allocated.

Repository

A place on a datastore resource which contains virtual machines.

SmartProxy

The SmartProxy is a software agent that acts on behalf of the CloudForms Management Engine Appliance to perform actions on hosts, providers, storage and virtual machines.

The SmartProxy can be configured to reside on the CloudForms Management Engine Appliance or on an ESX server version. The SmartProxy can be deployed from the CloudForms Management Engine Appliance, and provides visibility to the VMFS storage. Each storage location must have a SmartProxy with visibility to it. The SmartProxy acts on behalf of the CloudForms Management Engine Appliance. If the SmartProxy is not embedded in the CloudForms Management Engine server, it communicates with the CloudForms Management Engine Appliance over HTTPS (SSL) on standard port 443.

SmartState Analysis

Process run by the SmartProxy which collects the details of a virtual machine or instance. Such details include accounts, drivers, network information, hardware, and security patches. This process is also run by the CloudForms Management Engine server on hosts and clusters. The data is stored in the VMDB.

SmartTags

Descriptors that allow you to create a customized, searchable index for the resources in your clouds and infrastructure.

Storage Location

A device, such as a VMware datastore, where digital information resides that is connected to a resource.

Tags

Descriptive terms defined by a CloudForms Management Engine user or the system used to categorize a resource.

Template

A template is a copy of a preconfigured virtual machine, designed to capture installed software and software configurations, as well as the hardware configuration, of the original virtual machine.

Unmanaged Virtual Machine

Files discovered on a datastore that do not have a virtual machine associated with them in the VMDB. These files may be registered to a provider that the CloudForms Management Engine server does not have configuration information on. Possible causes may be that the provider has not been discovered or that the provider has been discovered, but no security credentials have been provided.

Virtual Machine

A software implementation of a system that functions similar to a physical machine. Virtual machines utilize the hardware infrastructure of a physical host, or a set of physical hosts, to provide a scalable and on-demand method of system provisioning.

Virtual Management Database (VMDB)

Database used by the CloudForms Management Engine Appliance to store information about your resources, users, and anything else required to manage your virtual enterprise.

Virtual Thumbnail

An icon divided into smaller areas that summarize the properties of a resource.

Zones

CloudForms Management Engine Infrastructure can be organized into zones to configure failover and to isolate traffic. Zones can be created based on your environment. Zones can be based on geographic location, network location, or function. When first started, new servers are put into the default zone.

1.4. Getting Help and Giving Feedback

If you experience difficulty with a procedure described in this documentation, visit the Red Hat Customer Portal at http://access.redhat.com. Through the customer portal, you can:

- search or browse through a knowledgebase of technical support articles about Red Hat products
- submit a support case to Red Hat Global Support Services (GSS)
- access other product documentation

Red Hat also hosts a large number of electronic mailing lists for discussion of Red Hat software and technology. You can find a list of publicly available mailing lists at https://www.redhat.com/mailman/listinfo. Click on the name of any mailing list to subscribe to that list or to access the list archives.

Documentation Feedback

If you find a typographical error in this manual, or if you have thought of a way to make this manual better, please submit a report to GSS through the customer portal.

When submitting a report, be sure to mention the manual's identifier: *Settings and Operations Guide*

If you have a suggestion for improving the documentation, try to be as specific as possible when describing it. If you have found an error, please include the section number and some of the surrounding text so we can find it easily.

[1] http://www.mozilla.org/en-US/firefox/organizations/faq/

Chapter 2. Settings Overview

To view and modify Configuration Options, hover over the **Configure** menu. Then, click on the type of setting you want to modify.

Configuration is divided into the following areas. The availability of each of these areas depends on the logged in user's account role. See Roles for more information.

- **My Settings** is available to all CloudForms Management Engine users. Its settings control the visual aspects of the console, time profiles, and tags used by the individual user.
- **Tasks** provides a list and status of jobs run by SmartProxies and jobs initiated from the console.
- **Configuration** is used to specify enterprise, region, zone, and server settings for the CloudForms Management Engine infrastructure. Diagnostics including logs and process status is also shown here.
- **SmartProxies** enables you to install and control SmartProxies that are installed on individual Hosts.
- **About** provides session information and links to CloudForms Management Engine documentation as well as the Red Hat Customer Portal.

Chapter 3. My Settings

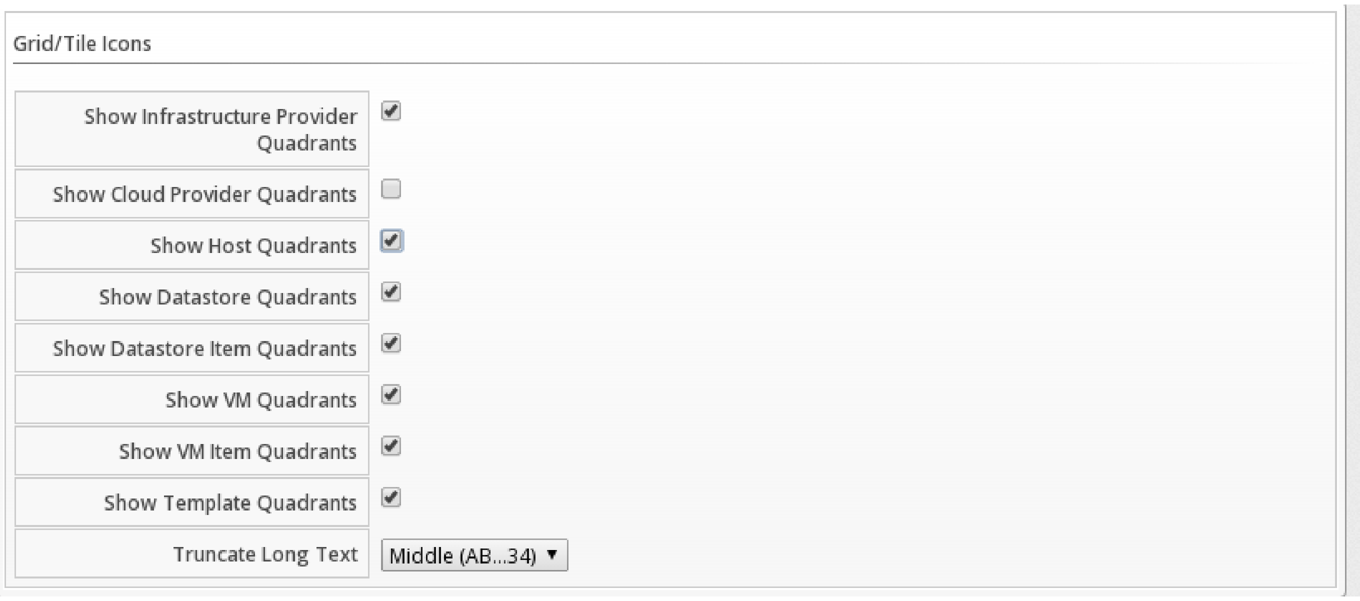
Options under **Configuration** → **My Settings** enable you to control user settings such as how things are displayed, default views, and individual tags. You can also set your color scheme, button options, and external RSS feeds on the main CloudForms Management Engine dashboard.

3.1. Visual Settings

For all of the **Visual** options, click **Save** to update your configuration settings. Click **Reset** to undo any unsaved changes that have been made on the current screen.

3.1.1. Grid and Tile Icons

This group of settings is used to control the view of your virtual thumbnails. Each thumbnail can be viewed as a single icon or as an icon with four quadrants. Use the quadrant view to see a component's properties at a glance.



Grid/Tile Icons

Show Infrastructure Provider Quadrants	☑
Show Cloud Provider Quadrants	□
Show Host Quadrants	☑
Show Datastore Quadrants	☑
Show Datastore Item Quadrants	☑
Show VM Quadrants	☑
Show VM Item Quadrants	☑
Show Template Quadrants	☑
Truncate Long Text	Middle (AB...34) ▼

- Check **Show Infrastructure Quadrants** to see the 4 icons in your provider. Uncheck to see only one icon.
- Check **Show Cloud Provider Quadrants** to see the 4 icons in your hosts. Uncheck to see only one icon.
- Check **Show Host Quadrants** to see the 4 icons in your hosts. Uncheck to see only one icon.
- Check **Show Datastore Quadrants** to see the 4 icons in your Datastores. Uncheck to see only one icon.
- Check **Show Datastore Item Quadrants** to see 4 icons, where applicable, in items inside a Datastore. Uncheck to see only one icon.
- Check **Show VM Quadrants** to see the 4 icons in your virtual machines. Uncheck to see only one icon.
- Check **Show VM Item Quadrants** to see 4 icons, where applicable, in items inside the virtual machines. Uncheck to see only one icon.

- Check **Show Template Quadrants** to see the 4 icons in your templates. Uncheck to see only one icon.
- Under **Truncate Long Text** to specify how you want names of items displayed if they are too long to show entirely. Select the option based on the pattern shown.

3.1.1.1. Changing Grid and Tile Icon Settings

Procedure 3.1. To Change Grid and Tile Icon Settings

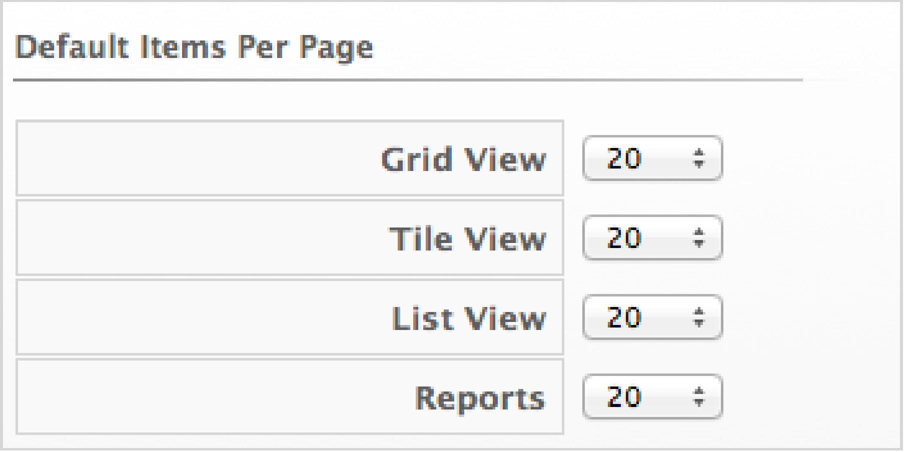
1. Navigate to **Configure** → **My Settings**, then click on the **Visual** tab.
2. In **Grid/Tile Icons**, check the items that you want to see all 4 quadrants for.
3. Click **Save**.

3.1.2. Setting Default Items Per Page

You can set the default number of items to display on each resource page.

Procedure 3.2. To Set Default Items Per Page

1. Navigate to **Configure** → **My Settings**, then click on the **Visual** tab.
2. In **Default Items Per Page** area, select the default number of items you want displayed for each view from the appropriate dropdown.



Default Items Per Page

Grid View	20
Tile View	20
List View	20
Reports	20

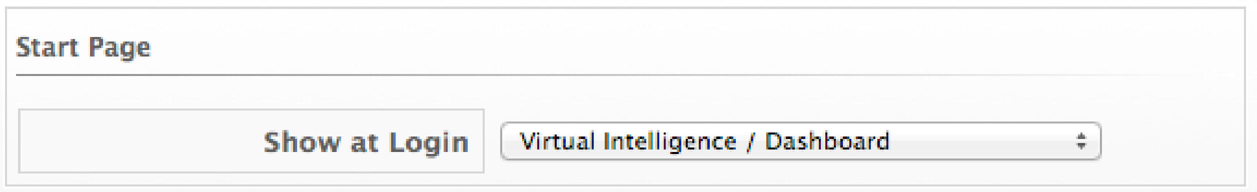
3. Click **Save**.

3.1.3. Setting the Start Page

You can set the default start page after logging in. For example, instead of going to the CloudForms Management Engine dashboard, you can set the default start page to see a list of your virtual machines.

Procedure 3.3. To Set the Start Page

1. Navigate to **Configure** → **My Settings**, then click on the **Visual** tab.
2. In the **Start Page** area, select the page you want to see at login.


Start Page

Show at Login: Virtual Intelligence / Dashboard

3. Click **Save**.

3.1.4. Setting Display Settings

You can set your own themes, colors, and time zone for the console. These settings are specific to the logged on user.

Procedure 3.4. To Set Display Settings

1. Navigate to **Configure** → **My Settings**, then click on the **Visual** tab.
2. Make selections from **Display Settings** for the following items.
   - Use **Header Accent Color** to select a color for your console header.
   - Use **Chart Theme** to select a group of colors and font sizes specifically for charts.
   - Use **Time Zone** to select in which time zone you want the console to display.

   > **Note**
   >
   > Note that in time zones where clocks are set forward for daylight savings time, the time zone correctly displays as EDT (Eastern Daylight Time) in the console. When the clocks are set back, it correctly displays as EST (Eastern Standard Time).

3. Click **Save**.

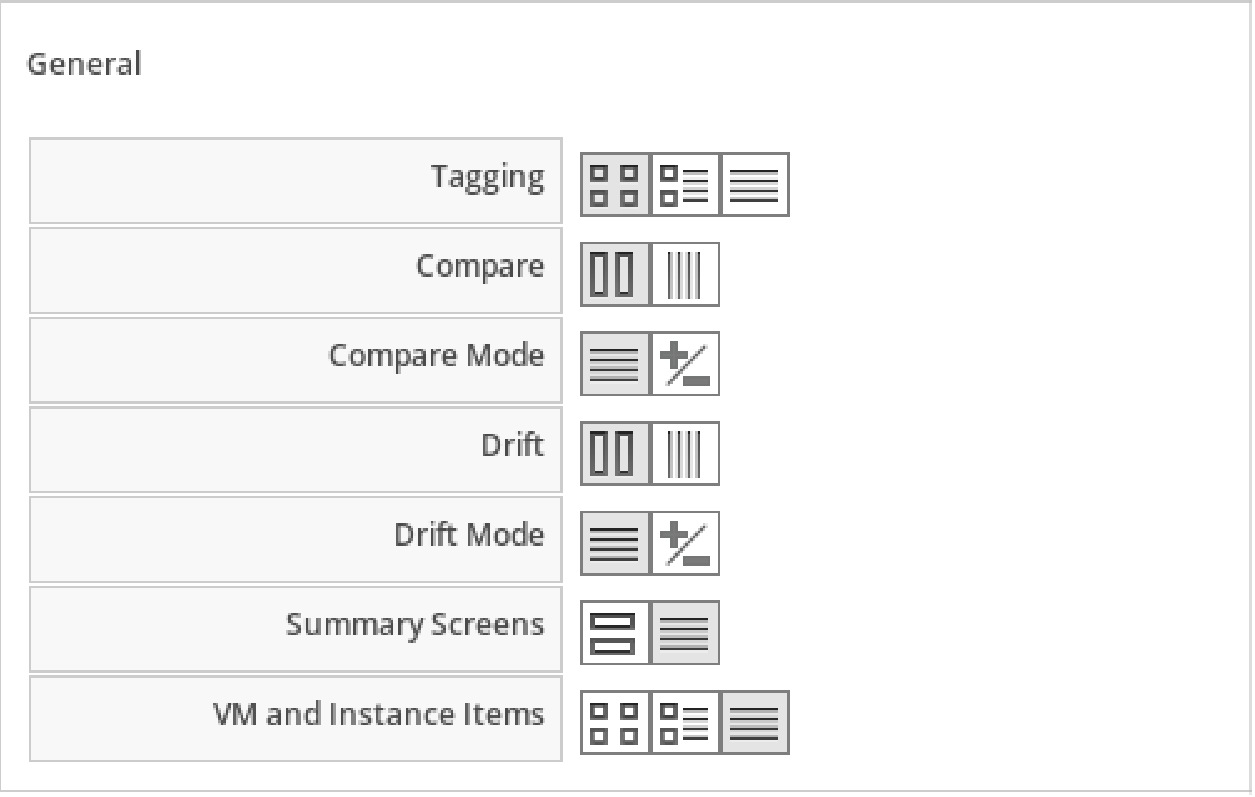
3.2. Default Views

You can decide on the default views for your virtual machines, infrastructure, and other pages where the view is customizable. These settings can also be controlled on the actual pages where the items appear.

3.2.1. Setting General View Options

Procedure 3.5. To Set General View Options

1. Navigate to **Configure** → **My Settings**, then click on the **Default Views** tab.
2. In the **General** area, click the appropriate button for the way you want to view each type of screen listed.



General

Tagging

Compare

Compare Mode

Drift

Drift Mode

Summary Screens

VM and Instance Items

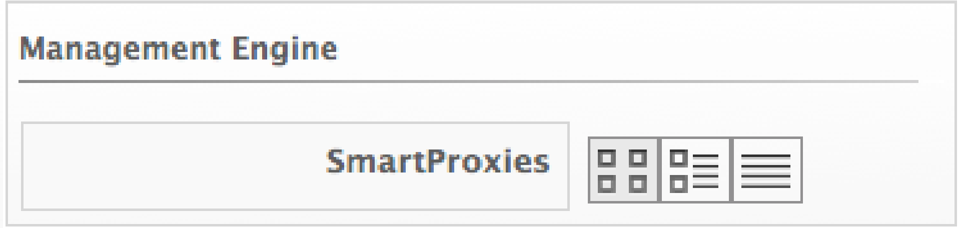
- Click ⊞ (**Grid View**) to view virtual thumbnails or icons
- Click ☷ (**Tile View**) for a view that combines the virtual thumbnail with some text properties that describe the items
- Click ☰ (**List View**) or ☰ (**Details Mode**) or ☰ (**Text View**) for a detailed textual listing of virtual machines
- Click ▯▯ (**Expanded View**) for an expanded view
- Click |||| (**Compressed View**) for a compressed view
- Click ± (**Exists Mode**) for an exists mode
- Click ⊟ (**Graphical View**) for a graphical view

3. Click **Save**.

3.2.2. Setting Default View for Management Engine

Procedure 3.6. To Set Default View for Management Engine

1. Navigate to **Configure** → **My Settings**, then click on the **Default Views** tab.
2. In the **Management Engine** area, click the button for the way you want to view SmartProxies.



Management Engine

SmartProxies

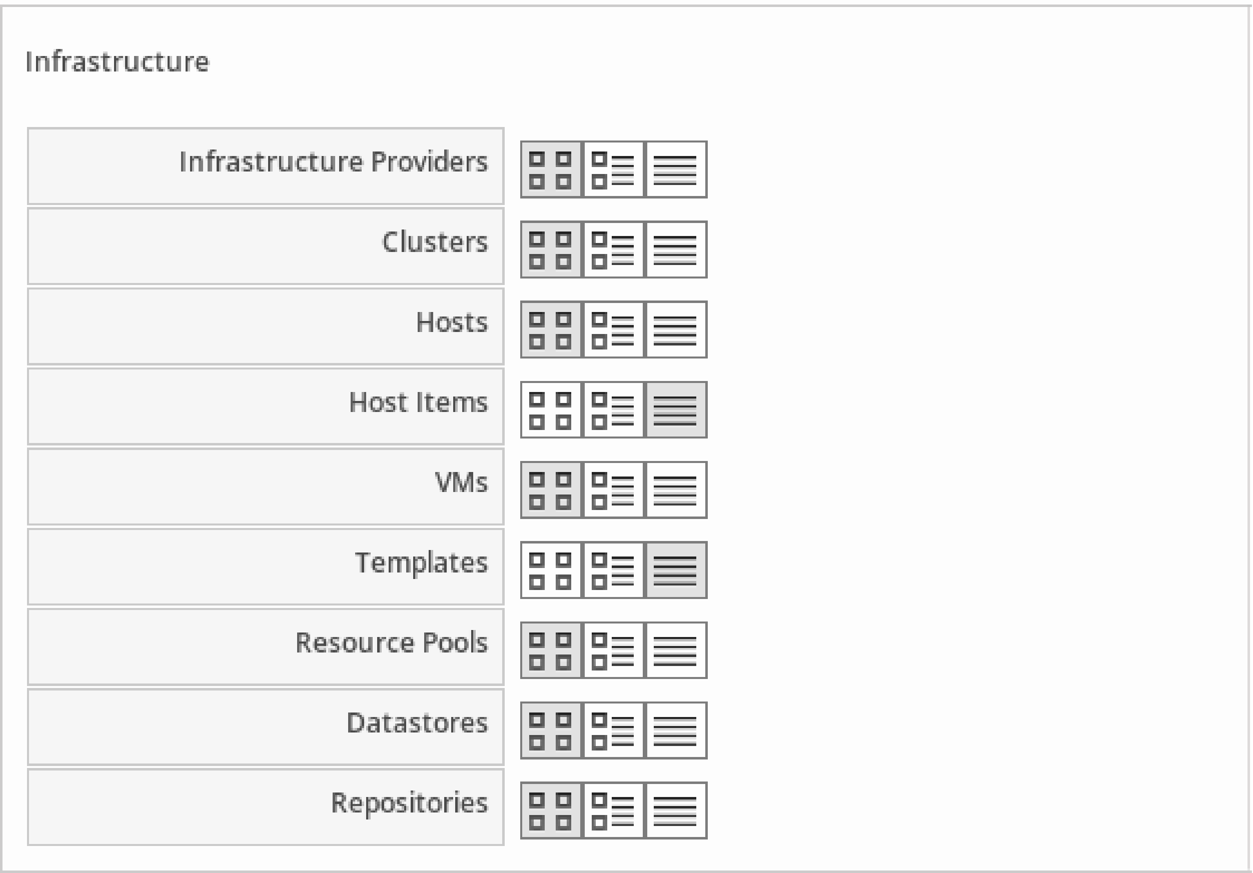
- Click ⊞ (**Grid View**) to view virtual thumbnails or icons
- Click ☷ (**Tile View**) for a view that combines the virtual thumbnail with some text properties that describe the items
- Click ☰ (**List View**) that provides a text listing of virtual machines

3. Click **Save**.

3.2.3. Setting Default Views for Infrastructure Components

Procedure 3.7. To Set Default Views for Infrastructure Components

1. Navigate to **Configure** → **My Settings**, then click on the **Default Views** tab.
2. In the **Infrastructure** area, click the appropriate button for the way you want to view each item.



Infrastructure

Infrastructure Providers

Clusters

Hosts

Host Items

VMs

Templates

Resource Pools

Datastores

Repositories

- Click ⊞ (**Grid View**) to view virtual thumbnails or icons

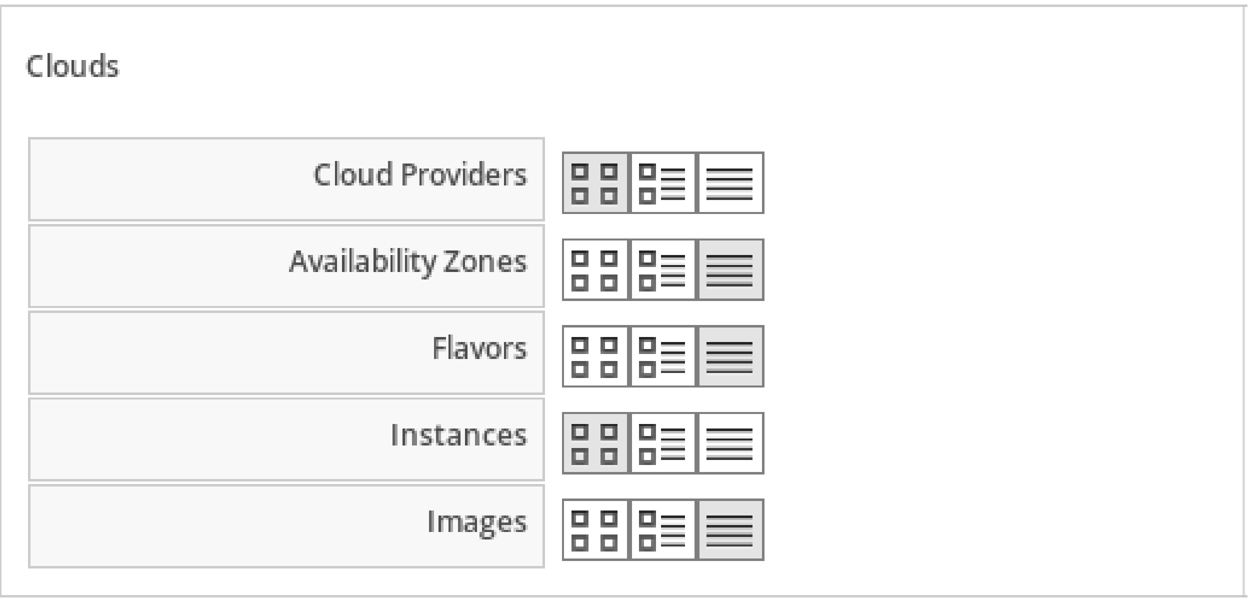
- Click (**Tile View**) for a view that combines the virtual thumbnail with some text properties that describe the items
- Click (**List View**) that provides a text listing of virtual machines

3. Click **Save**.

3.2.4. Setting Default Views for Clouds

Procedure 3.8. To Set Default Views for Clouds

1. Navigate to **Configure** → **My Settings**, then click on the **Default Views** tab.
2. In the **Clouds** area, click the button for the way you want to view each item.



Clouds

Cloud Providers	●	○	○
Availability Zones	○	○	●
Flavors	○	○	●
Instances	●	○	○
Images	○	○	●

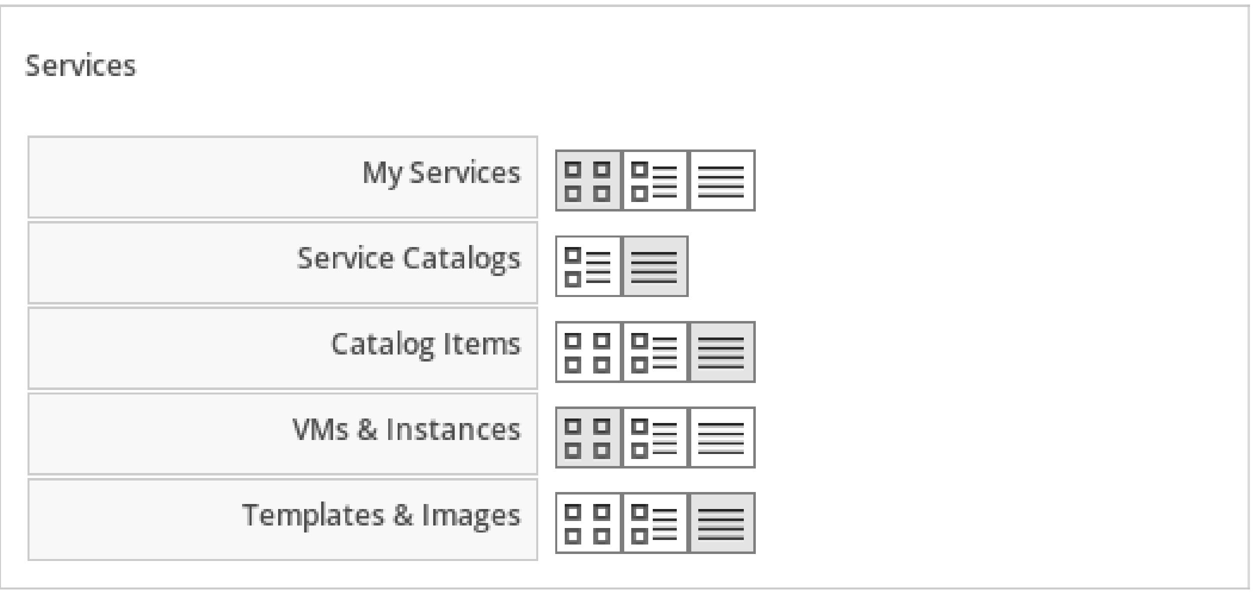
- Click (**Grid View**) to view virtual thumbnails or icons
- Click (**Tile View**) for a view that combines the virtual thumbnail with some text properties that describe the items
- Click (**Detail View**) that provides a text listing of virtual machines

3. Click **Save**.

3.2.5. Setting Default Views for Services

Procedure 3.9. To Set Default Views for Services

1. Navigate to **Configure** → **My Settings**, then click on the **Default Views** tab.
2. In the **Services** area, click the appropriate button for the way you want to view each item.



Services

My Services

Service Catalogs

Catalog Items

VMs & Instances

Templates & Images

- Click ⊞ (**Grid View**) to view just virtual thumbnails or icons
- Click ☷ (**Tile View**) for a view that combines the virtual thumbnail with some text properties that describe the items
- Click ☰ (**Detail View**) that provides a text listing of virtual machines

3. Click **Save**.

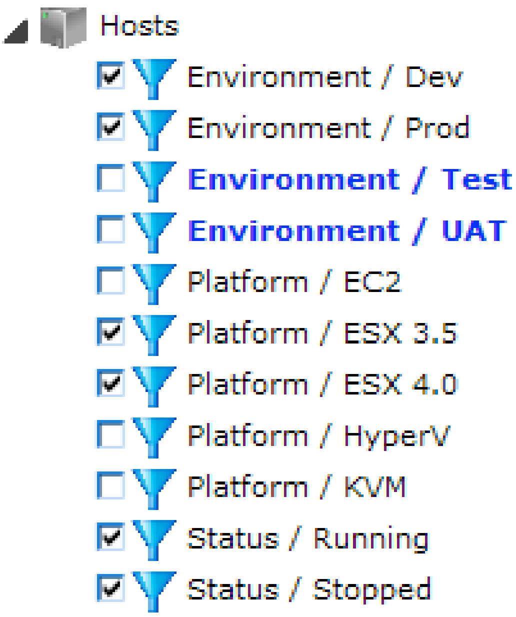
3.3. Default Filters

You can set the default filters displayed for your hosts, virtual machines, and templates. These settings are available to all users.

3.3.1. Setting Default Filters for Hosts

Procedure 3.10. To Set Default Filters for Hosts

1. Navigate to **Configure** → **My Settings**, then click on the **Default Filters** tab.
2. From the **Hosts** folder, check the boxes for the default filters that you want available on the Hosts page. (Not all filters are listed in the figure below.) Items that have changed will show in blue, bold text.



Hosts
- ☑ Environment / Dev
- ☑ Environment / Prod
- □ **Environment / Test**
- □ **Environment / UAT**
- □ Platform / EC2
- ☑ Platform / ESX 3.5
- ☑ Platform / ESX 4.0
- □ Platform / HyperV
- □ Platform / KVM
- ☑ Status / Running
- ☑ Status / Stopped

3. Click **Save**.

3.3.2. Setting Default Filters for Templates

Procedure 3.11. To Set Default Filters for Templates

1. Navigate to **Configure** → **My Settings**, then click on the **`Default Filters`** tab.

2. From the **`Templates and Images`** folder, check the boxes for the default filters that you want available. Items that have changed show in blue and bold text.

3. Click **Save**.

3.3.3. Setting Default Filters for Virtual Machines

Procedure 3.12. To Set Default Filters for Virtual Machines

1. Navigate to **Configure** → **My Settings**, then click on the **`Default Filters`** tab.

2. From the **`VMs and Instances`** folder, check the boxes for the default filters that you want available. Items that have changed show in blue and bold text.

3. Click **Save**.

3.4. Time Profiles

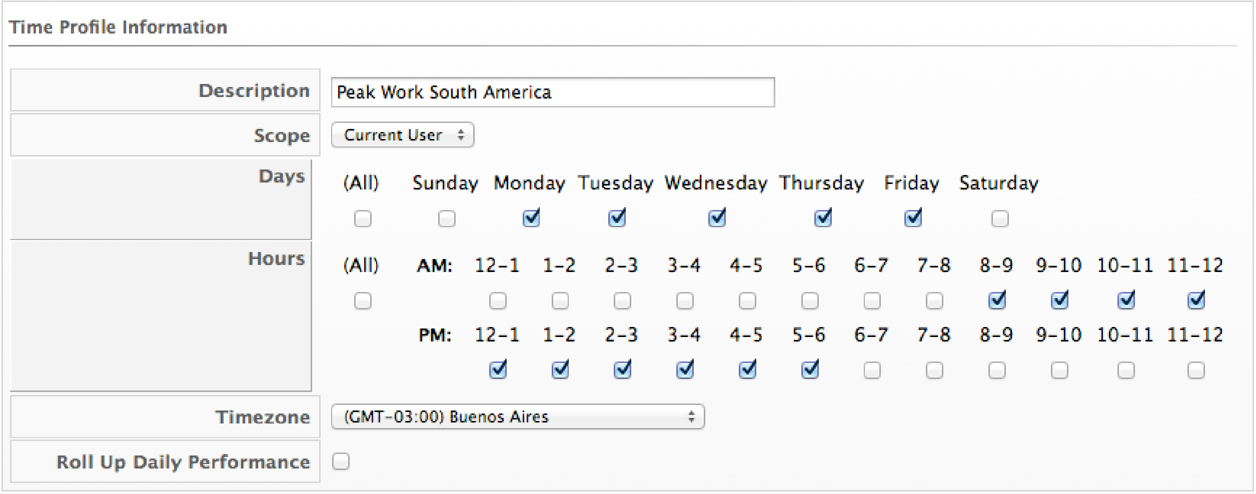
Time profiles limit the hours for which data is displayed when viewing capacity and utilization screens. They are also used for performance and trend reports, and for **Optimize** pages.

3.4.1. Creating a Time Profile

Procedure 3.13. To Create a Time Profile

1. Navigate to **Configure** → **My Settings**, then click on the **`Time Profiles`** tab.

2. Click ⚙ (**`Configuration`**), and + (**`Add a new Time Profile`**).



Time Profile Information

Description	Peak Work South America
Scope	Current User
Days	(All) ☐ Sunday ☐ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☐
Hours	(All) ☐ AM: 12-1 ☐ 1-2 ☐ 2-3 ☐ 3-4 ☐ 4-5 ☐ 5-6 ☐ 6-7 ☐ 7-8 ☐ 8-9 ☑ 9-10 ☑ 10-11 ☑ 11-12 ☑ PM: 12-1 ☑ 1-2 ☑ 2-3 ☑ 3-4 ☑ 4-5 ☑ 5-6 ☑ 6-7 ☐ 7-8 ☐ 8-9 ☐ 9-10 ☐ 10-11 ☐ 11-12 ☐
Timezone	(GMT-03:00) Buenos Aires
Roll Up Daily Performance	☐

3. Type a meaningful name in the **Description** field.

4. For **Scope**, select **All Users** to create a global time profile available to all users. Only the super administration and administration roles can create, edit, and delete a global profile. Select **Current User** if this time profile should only be available to the user creating it.

5. Check the **Days** and **Hours** for the time profile.

6. For **Time zone**, you can select a specific time zone or, you can let the user select a time zone when displaying data.

7. If you select a specific time zone, you also have the option to **Roll Up Daily Performance** data. This option is only available to users with the administration or super administration role. Enabling the **Roll Up Daily Performance** option reduces the time required to process daily capacity and utilization reports and to display daily capacity and utilization charts.

8. Click **Add**.

Note

The following relationships exist between time zones and performance reports:

- The configured time zone in a performance report is used to select rolled up performance data, regardless of the user's selected time zone.
- If the configured time zone is null, it defaults to UTC time for performance reports.
- If there is no time profile with the report's configured time zone that is also set to roll up capacity and utilization data, the report does not find any records.

For non-performance reports, the user's time zone is used when displaying dates and times in report rows.

3.4.2. Editing a Time Profile

Procedure 3.14. To Edit a Time Profile

1. Navigate to **Configure** → **My Settings**, then click on the **Time Profiles** tab.

2. Check the time profile you want to edit.

3. Click ⚙ (**Configuration**), and ✏ (**Edit Selected Time Profile**).

4. Make the required changes.

5. Click **Save**.

3.4.3. Copying a Time Profile

Procedure 3.15. To Copy a Time Profile

1. Navigate to **Configure** → **My Settings**, then click on the **Time Profiles** tab.

2. Check the time profile you want to copy.

3. Click ⚙ (**Configuration**), and ⧉ (**Copy Selected Time Profile**).

4. Make the required changes.

5. Click **Save**.

3.4.4. Deleting a Time Profile

Procedure 3.16. To Delete a Time Profile

1. Navigate to **Configure** → **My Settings**, then click on the **Time Profiles** tab.

2. Check the time profile you want to edit.

3. Click ⚙ (**Configuration**), and 🗑 (**Delete Selected Time Profile**).

4. Make the required changes.

5. Click **Save**.

Chapter 4. Tasks

The SmartProxy and console create virtual machine SmartState Analysis tasks that can be tracked through the console. The status of each task is displayed including time started, time ended, what part of the task is currently running, and any errors encountered.

4.1. My VM Analysis Tasks

All tasks run by SmartProxies are tracked under the **VM Analysis Tasks** page.

From My VM Analysis Tasks, you can:

- See jobs that the logged on user created for the SmartProxy either through a schedule or by manually initiating a SmartState Analysis of a virtual machine.
- See if a job completed successfully, resulted in an error, or is running.
- See the reason for an error.
- Filter the tasks by status and state.
- View the owner or host of the virtual machine referenced.
- Delete a task either explicitly or older than another task.

> **Note**
>
> If you are logged on as super administrator, you can see all tasks started by any user, including the internal user, from **Assistance** → **Diagnostics**

4.1.1. Viewing SmartProxy Tasks

Procedure 4.1. To View SmartProxy Tasks

1. Navigate to **Configure** → **Tasks**, then click on the **VM Analysis Tasks** tab.
2. Click on a row to be taken to the detail page for the resource referenced in the task.

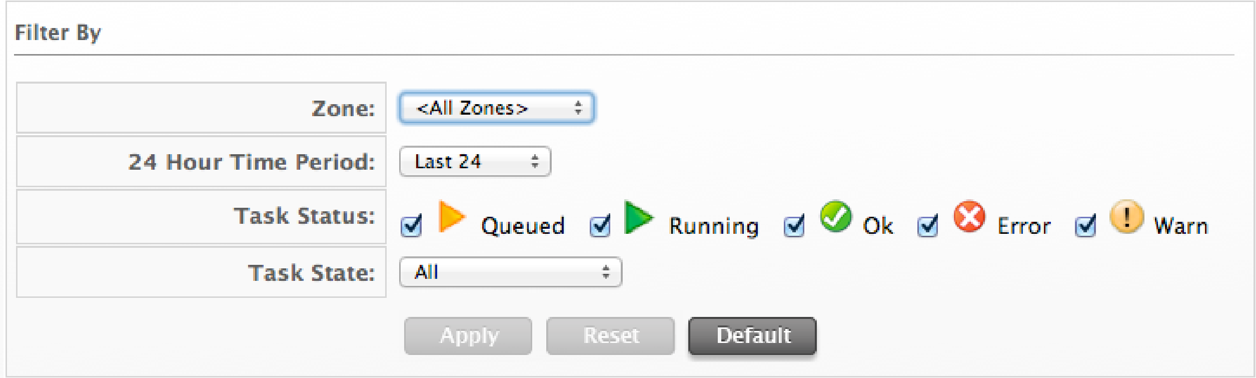
> **Note**
>
> You can filter the task list by **Zone**, **24 Hour Time Period**, **Task Status**, and **Task State**.

4.1.2. Filtering the VM Analysis Task List

This procedure describes how to filter VM analysis task lists. You can filter the task list by zone, time period, task status, and task state.

Procedure 4.2. To Filter the VM Analysis Task List

1. Navigate to **Configure** → **Tasks**, then click on the **My VM Analysis Tasks** tab.



Filter By

Zone: <All Zones>

24 Hour Time Period: Last 24

Task Status: ☑ Queued ☑ Running ☑ Ok ☑ Error ☑ Warn

Task State: All

2.
   - From **Zone**, select either a specific zone or **All Zones**.
   - From **24 Hour Time Period**, select the period of time to view the tasks.
   - For **Task Status**, check the boxes next to the status you want to view.
   - From the **Tasks State** dropdown, select the state you want to view.
3. Click **Apply**.

4.1.3. Deleting VM Analysis Tasks

Procedure 4.3. To Delete VM Analysis Tasks

1. Navigate to **Configure** → **Tasks**, then click on the **My VM Analysis Tasks** tab.
2. Check the boxes for the tasks you want to delete.
3. Click 🗑 (**Delete Tasks**), and then 🗑 (**Delete**).
4. Click **OK** to confirm.

4.1.4. Deleting VM Analysis Tasks Older than a Specific Task

Procedure 4.4. To Delete VM Analysis Tasks Older than a Specific Task

1. Click **Configure** → **Tasks**.
2. Click the **My VM Analysis Tasks** tab.
3. Check the box for the task you want to delete tasks older than.
4. Click 🗑 (**Delete Tasks**), and then 🗑 (**Delete Older**).
5. Click **OK** to confirm.

4.2. Viewing UI Tasks

Procedure 4.5. To View UI Tasks

- Navigate to **Configure** → **Tasks**, then click on the **My Other UI Tasks** tab.

Note

You can also filter your tasks. See *Filtering the UI Task List*.

4.2.1. Filtering a UI Task List

This procedure describes how to filter tasks. You can filter a task list by time period, task status, and task state.

Procedure 4.6. To Filter a UI Task List

1. Navigate to **Configure** → **Tasks**, then click on the **My Other UI Tasks** tab.
2. From the **24 Hour Time Period** dropdown, select the period of time to view the tasks.
3. For **Task Status**, check the boxes next to the status you want to view.
4. From the **Tasks State** dropdown, select the state you want to view.
5. Click **Apply**.

4.2.2. Deleting UI tasks

Procedure 4.7. To Delete UI Tasks

1. Navigate to **Configure** → **Tasks**, then click on the **My Other UI Tasks** tab.
2. Check the boxes for the tasks you want to delete.
3. Click 🗑 (**Delete Tasks**), and then 🗑 (**Delete**).
4. Click **OK** to confirm.

4.2.3. Deleting UI Tasks Older than a Specific Task

Procedure 4.8. To Delete UI Tasks Older than a Specific Task

1. Navigate to **Configure** → **Tasks**, then click on the **My Other UI Tasks** tab.
2. Check the box for the task you want to delete tasks older than.
3. Click 🗑 (**Delete Tasks**), and then 🗑 (**Delete Older**).
4. Click **OK** to confirm.

4.3. All Tasks

If you are logged on as super administrator or administration, you can see all tasks started by any user, including the internal user, from **Configure** → **Tasks**, then clicking on the **All VM Analysis Tasks** or **My Other UI Tasks** pages.

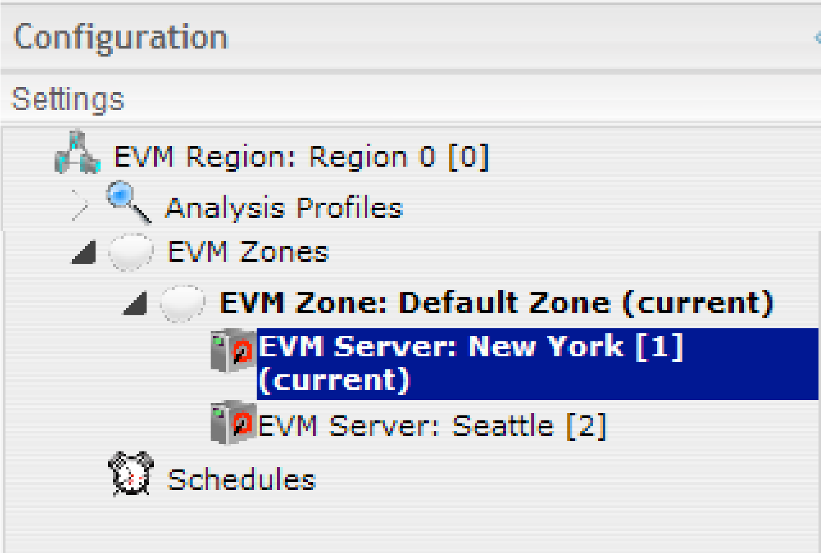
Chapter 5. Configuration

From the **Configuration** area, you can specify operating parameters for the CloudForms Management Engine infrastructure, view diagnostic information, and analytics on the servers. The accordion menu shows your CloudForms Management Engine infrastructure at the enterprise, zone, and server levels. There are three main areas.

- **Settings** enable you to modify the configuration of your CloudForms Management Engine infrastructure. You can also create analysis profiles and schedules for these profiles.
- **Diagnostics** dsiplays the status of your servers and their roles and provides access to logs.

5.1. Settings

Under **Configure** → **Configuration**, then in the **Settings** accordion, you have a hierarchy of the configurable items in your CloudForms Management Engine architecture. At the top level, you have **Settings** including users, LDAP Groups, account roles, capacity and utilization collection, tag categories, values, and imports, custom variable imports, and license uploads. When you click on **Settings** and expand it, you can configure **Analysis Profiles**, **Zones**, and **Schedules**.



When you go the **Settings** area, you are automatically taken to the server list under **Zones**.

5.1.1. Regions

5.1.1.1. Region Settings

In the **Region** area, set items that apply to your entire CloudForms Management Engine infrastructure such as users, LDAP Groups, capacity and utilization collection, company tags and tag categories, and licensing. Regions are also used for database replication.

5.1.1.2. About Regions

Regions are used to consolidate data from multiple VMDBs to a central database. The database at the top level, the master VMDB, cannot be used for operational tasks such as

SmartState Analysis or Capacity and Utilization data collection. It is intended for use as a reporting database that includes all information across multiple subordinate regions. The subordinate regions replicate their information to the master. Note that the subordinate regions are not aware of each other from a database perspective. That is, you will not see information from one subordinate region in another. The only VMDB with data visibility to all subordinate regions is the top level.

Masters Regions Scope

- Reports all information from all subordinate VMDBs reporting up to it
- Can perform power operations on virtual machines from subordinate regions
- Controls its own access control list

Subordinate Regions Scope

- Each subordinate controls its own access control independent of the other regions
- Can only do work (such as SmartState Analysis and Capacity and Utilization collection) in its own region
- Has no knowledge of the other regions
- Replicates its data up to the master region

5.1.1.3. Capacity and Utilization Collections

5.1.1.3.1. Capacity and Utilization Collection Settings

Use **C & U Collection Settings** to select specifically which clusters and datastores you want to collect usage data for. By selecting a cluster, you are choosing to collect data for all hosts and virtual machines that are part of that cluster. You must also have a server with the Capacity & Utilization Coordinator, Data Collector, and Data Processor roles enabled as well. See *Server Control Settings*.

After a provider has been discovered and its relationships refreshed, the clusters, hosts, and datastores show under **Configure** → **Configuration**, then by clicking on the **Settings** accordion, then **Region**, then by clicking on the **C & U Collection** tab.

5.1.1.3.2. Enabling a Cluster, Host, or Datastore for Capacity and Utilization Collection

Procedure 5.1. To Enable a Cluster, Host, or Datastore for Capacity and Utilization Collection

1. Navigate to **Configure** → **Configuration**, then click on the **Settings** accordion.
2. Select **Region**, then click on the **C & U Collection** tab.
3. In the **Clusters** area, check all clusters and hosts that you want to collect data for.
4. In the **Datastores** area, check all datastores that you want to collect data for.
5. Click **Save**.

Note

As new clusters, hosts, and datastores are discovered, you will need to come back to this configuration to enable collection of capacity and utilization data unless you have used the `Collect for All` check boxes

5.1.1.4. Tags

5.1.1.4.1. Company Tag Categories and Tags

CloudForms Management Engine allows you to create your own set of tags and tag categories. Use tags to create a customized, searchable index for your resources. Depending on your database type, your tags may be case sensitive. After creating these values, you can apply them to your resources. There are two kinds of tags.

- Company tags which you will see under **My Company Tags** for a resource. Create company tags by navigating to **Configure** → **Configuration**, then clicking on the **Settings**, then selecting **Region**, then the **My Company Tags** tab. A selection of company tags is provided to you by default as samples. These can be deleted if you do not need them, but are not recreated by CloudForms Management Engine.
- System tags are assigned automatically by CloudForms Management Engine.

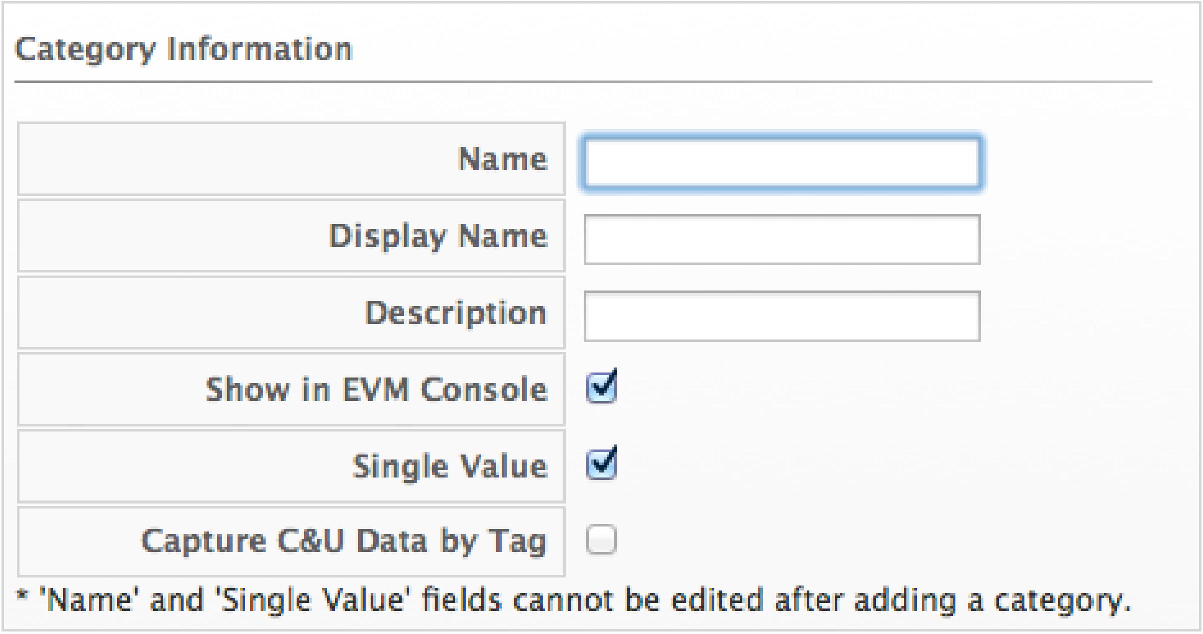
Note

If you entered a **Company Name** under **Configure** → **Configuration**, then clicking on the **Settings** tab, then the Server your desired server, that name will appear on the tab instead of **My Company**.

5.1.1.4.2. Creating a Tag Category

Procedure 5.2. To Create a Tag Category

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then **Region**, then click on the **My Company Categories** tab.
3. Click ✚ (**Click to add a new category**).
4. In the **Category Information** area,



Category Information

Name	
Display Name	
Description	
Show in EVM Console	☑
Single Value	☑
Capture C&U Data by Tag	□

* 'Name' and 'Single Value' fields cannot be edited after adding a category.

- Use **Name** to create a short name that refers to category in the VMDB.

> **Note**
>
> The **Name** and **Single Value** fields cannot be changed after the category has been added.

- Use **Display Name** to specify how you want to see the name of the category in the Console.
- Use **Description** to type a brief explanation of how the category should be used. This shows when you try to add a value to the category.
- Check **Show in Console** when you feel that the category is ready for use in the console. For example, you want to populate values for the category before exposing it to users.
- Check **Single Value** for categories that can only have a single value assigned to a resource. For example, a virtual machine can only be assigned to one location, but could belong to more than one department.
- Check **Capture C & U Data** by tag to be able to group capacity and utilization data by this tag category. To use this, be sure to assign this tag to all the resources that you want to group by.

5. Click **Add**.

Result:

Repeat these steps for each category you need. After you have created the category, you can add values to it.

> **Important**
>
> If no values are created for a category, you are unable to assign a value from that category nor be able to filter by that category.

5.1.1.4.3. Deleting a Tag Category

Procedure 5.3. To Delete a Tag Category

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then **Region**, then click on the **My Company Categories** tab.
3. Click 🗑 (**Delete this category**) next to the category to delete it.

> **Note**
>
> When you delete a tag category, the category values are removed, and any tags from the category are unassigned from all resources.

5.1.1.4.4. Creating a Company Tag

Procedure 5.4. To Create a Company Tag

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then **Region**, then click on the **My Company Tags** tab.
3. In the **Choose a Category** area, select a category from the **Category** dropdown.

   Note that some categories only allow one value to be assigned to a resource.

   > **Note**
   >
   > For some databases such as **PostgreSQL**, tags are case sensitive. For example, filtering by **Linux** in title case give you different results from filtering by **linux** in lower case.

4. Click + (**New Entry**), and type a **Name** and **Display Name** for your new value.
5. Click (**Add this entry**) to confirm the entry.
6. Repeat these steps for each value you need.

5.1.1.4.5. Deleting a Company Tag

Procedure 5.5. To Delete a Company Tag

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then **Region**, then click on the **My Company Tags** tab.
3. Click 🗑 (**Click to delete this entry**) next to the tag to delete it.

> **Note**
>
> When you delete a tag, the tag is also deleted from any resource to which it was assigned.

5.1.1.4.6. Importing Tags for Virtual Machines

You can import a CSV file with tag assignments into the VMDB. For the import to be successful, be aware of the following:

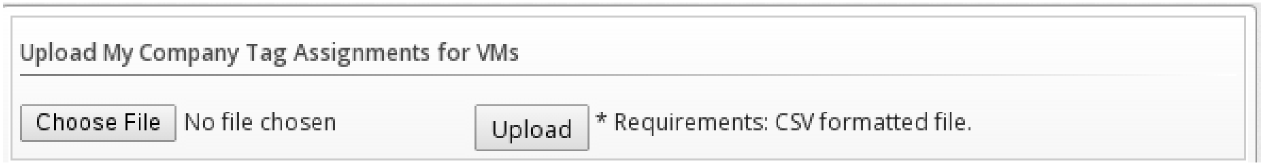
- The file must be in the following format, with one line for each virtual machine. One virtual machine per tag must be on a separate line even if you are assigning multiple tags of the same category.
- You must use the display names of the category and the display name for the tag for the import to work.

```
name,category,entry
evm2,Provisioning Scope,All
evm2,Exclusions,Do not Analyze
evm2,EVM Operations,Analysis Successful
rhel6,Department,Presales
rhel6,Department,Support
```

5.1.1.4.7. Importing Tags for a Virtual Machine from a CSV File

Procedure 5.6. To Import Tags for a Virtual Machine from a CSV File

1. Make sure the CSV file is in the required format.
2. Navigate to **Configure** → **Configuration**.
3. Click on the **Settings** accordion, then **Region**, then click on the **Import Tags** tab.
4. Click **Choose File** to go to the location where the file is located.



Upload My Company Tag Assignments for VMs

* Requirements: CSV formatted file.

5. Click **Upload**.

> **Note**
>
> If there are any problems with the file, such as an incorrect column name, unknown virtual machine, unknown tag, or multiple values for a tag that should have only one, an error message will appear in the console for those records.

6. Click **Apply**.

5.1.1.4.8. Importing Custom Values for Virtual Machines and Hosts

You can import a CSV file with asset tag information into the VMDB for a virtual machine or import custom values for hosts. For the import to be successful, the file must be in the following format, with one line for each virtual machine or host.

- There are two columns
- The first line of the file must have the column names as shown below
- The column names are case sensitive
- Each value must be separated by a comma

Virtual Machine Import Example

```
name,custom_1
Ecommerce,665432
Customer,883452
SQLSrvr,1090430
Firewall,8230500
```

For virtual machines, the value for custom_1 will show in the **VM Summary** page as the **Custom Identifier** in the **Properties** area. All of the custom values will show in the **Custom Fields** area.

Host Import Example

```
hostname,custom_1,custom_2
esx303.galaxy.local,15557814,19948399
esxd1.galaxy.local,10885574,16416993
esxd2.galaxy.local,16199125,16569419
```

For hosts, the value for custom_1 will show in the **Host Summary** page as the **Custom Identifier** in the **Properties** area. All of the custom values will show in the **Custom Fields** area.

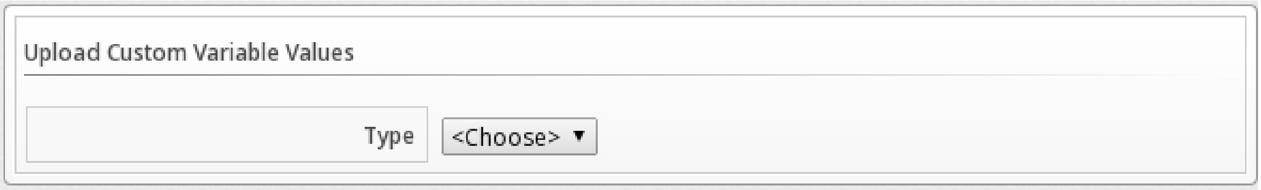
5.1.1.4.9. Importing Asset Tags for a Virtual Machine from a CSV File

Procedure 5.7. To Import Asset Tags for a Virtual Machine from a CSV File

1. Make sure the CSV file is in the required format.
2. Navigate to **Configure** → **Configuration**.

3. Click on the **Settings** accordion, then **Region**, then click on the **Import** tab.

4. Select the type of custom variable you want to import, either **Host** or **VM**.



Upload Custom Variable Values

Type <Choose>

5. Click **Browse** to go to the location where the custom variable file is located.

6. Click **Upload**.

Note

If there are any problems with the file, such as an incorrect column name, unknown virtual machine or host, a message appears.

7. Click **Apply**.

5.1.1.5. Registering and Updating CloudForms Management Engine

The **Red Hat Updates** page enables you to edit customer information, register appliances, and update appliances. Editing customer information enables you to determine the registration point, User ID, and password. CloudForms prompts you to update the Server URL when updating the registration point to a local Red Hat Satellite. The **Status of Available Servers** area provides options to refresh, register, check for updates, and to update. The Red Hat Updates page enables the Content Delivery Network (CDN) to assign the necessary update packages to the CloudForms Management Engine Server.

Using the **Check For Updates** task button, the CDN assigns any necessary update packages to your server and notifies you. Click **Update** and the CloudForms Management Engine packages install and update.

Three steps are required for updating the CloudForms Management Engine Appliance:

1. Register the CloudForms Management Engine for updates if it is not already registered.

2. Update the CloudForms Management Engine Appliance.

3. Update other system packages.

The following tools are used during the update process:

- **Yum** provides package installation, updates, and dependency checking.
- **Red Hat Subscription Manager** manages subscriptions and entitlements.
- **Red Hat Satellite Server** runs at customer locations providing local system registration and updates from inside the customer's firewall.

Important

The update worker synchronizes the VMDB with the status of available CloudForms Management Engine content every 12 hours.

Note

Servers with the **`RHN Mirror`** role also act as a repository for other Appliances to pull CloudForms Management Engine packages updates.

5.1.1.5.1. Editing Customer Information

The **`Red Hat Updates`** page enables you to edit customer information.

Procedure 5.8. To Edit Customer Information

1. Navigate to **Configure** → **Configuration**. Select **Region** in the accordian menu and click the **Red Hat Updates** tab.

2. Click **`Edit Registration`**.

3. The Customer Information area displays options to edit registration, User ID and Password.

   - **`Register to`** field provides options for the Customer Portal, RHN Satellite v5 for Red Hat Satellite 5.x servers, and RHN Satellite v6 for Red Hat Satellite 6.x servers. If switching to RHN Satellite v5 or v6, the page will refresh and a prompt for a Server URL will be included in the Customer Information area.

   - The HTTP Proxy area displays options to enable usage of the HTTP Proxy.

   - The **`User ID`** and **`Password`** are the customer account details for the Customer Portal or Satellite.

5.1.1.5.2. Registering Appliances

The **`Red Hat Updates`** page enables you to register appliances.

Procedure 5.9. To Register a CloudForms Management Engine Appliance

1. Navigate to **Configure** → **Configuration**. Select **Region** in the accordian menu and click the **Red Hat Updates** tab.

2. Click **`Edit Registration`**. Three options are available for registering the CloudForms Management Engine Appliance:

Option	Use
Red Hat Subscription Management	Registers to the Red Hat hosted server (**`subscription-manager`** commands). Due to dependency issues, you must enable the CloudForms repo to use this option. To enable the repo, open a terminal to the appliance and run **`yum-config-manager --enable cf-me-5.3-for-rhel-6-rpms`**.

Option	Use
Red Hat Satellite 5	Registers to a Satellite 5 server that you have installed inside your firewall (**rhn** commands). This option is recommended for large, multi-appliance CloudForms Management Engine deployments.
Red Hat Satellite 6	Register to a Satellite 6 server (pending release) that you have installed inside your firewall (**subscription-manager** commands).

5.1.1.5.3. Updating Appliances

The **Red Hat Updates** page enables you to check for updates and update registered appliances.

Procedure 5.10. To Update a CloudForms Management Engine Appliance

1. Navigate to **Configure** → **Configuration**. Select **Region** in the accordian menu and click the **Red Hat Updates** tab.

2. After registering, the following options are available in the **Appliance Updates** section of the **Red Hat Updates** tab:

Option	Use
Check for Updates	Checks for available updates using **yum**.
Register	Attempts to register the appliance if it is not already registered. CloudForms Management Engine subscribes to the **rhel-x86_64-server-6-cf-me-3** RHN channel for RHN registered appliances, and to the products designated by Red Hat product certification for **subscription-manager** registered appliances. The Red Hat Enterprise Linux channels are enabled by default on registration. In addition, CloudForms Management Engine checks for updates after registering.
Apply CFME Update	Applies updates to CloudForms Management Engine packages only. Specifically, this option runs the **yum -y update cfme-appliance** command. This command installs every package listed in the dependency tree if it is not already installed. If a specific version of a package is required, that version of the package is installed or upgraded. No other packages, such as PostgreSQL or Red Hat Enterprise Linux, are updated.

5.1.2. Profiles

5.1.2.1. Creating an Analysis Profile

You can create an analysis profile by referring to the sample profiles provided in the console. You can copy the sample profile or create a new one.

5.1.2.2. Creating a Host Analysis Profile

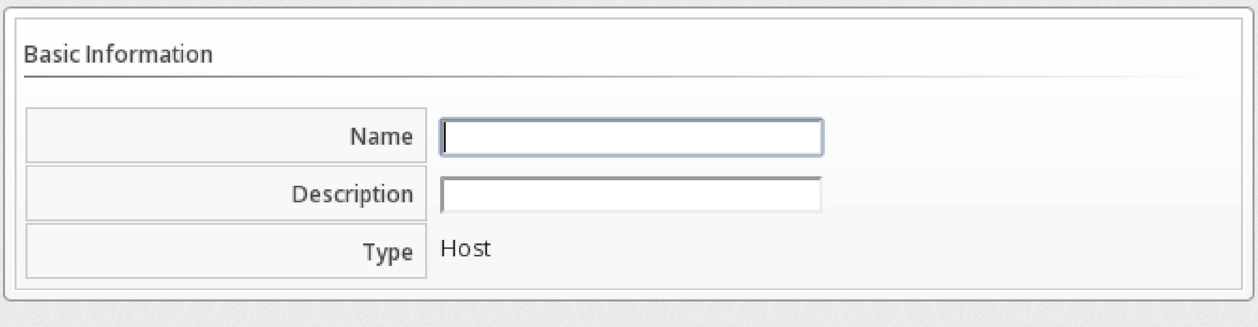
Procedure 5.11. To Create a Host Analysis Profile

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Settings** accordion, then click **Analysis Profiles**.

3. Click ⚙ (**Configuration**), and + (**Add Host Analysis Profile**).

4. In the **Basic Information** area, type in a **Name** and **Description** for the analysis profile.

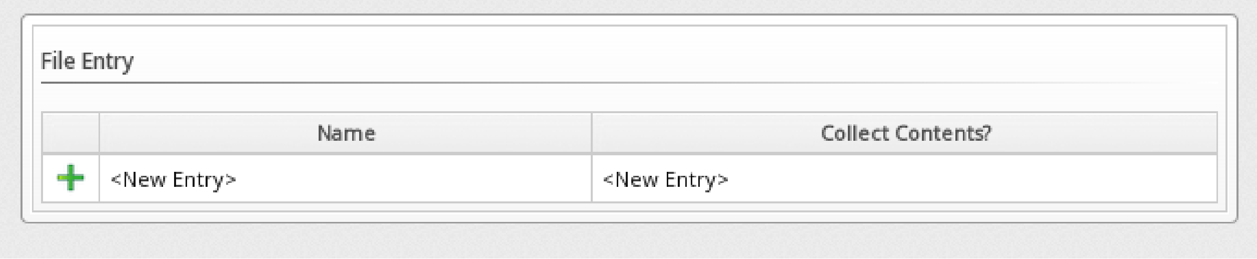


Basic Information

Name	
Description	
Type	Host

5. Click **File** to collect information about a file or group of files.

6. From the **File Entry** area, click + (**Click to add a new entry**) to add a file or group of files.



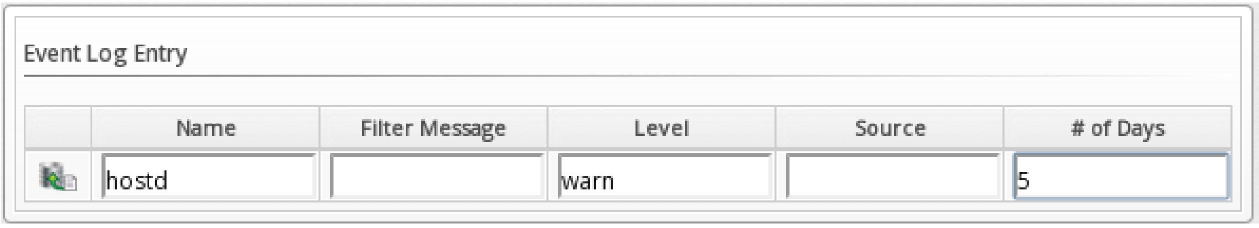
File Entry

	Name	Collect Contents?
+	<New Entry>	<New Entry>

- Check **Collect Contents** to not only check for existence, but also gather the contents of the file. If you do this, then you can use the contents to create policies in CloudForms Management Engine Control. See the *CloudForms Management Engine Control Guide*.

7. Click **Event Log** to specify event log entries to collect.

8. From the **Event Log Entry** area, click + (**Click to add a new entry**) to add a type of event log entry. Type in a **Name**. You can type in a specific message to find in **Filter Message**. In **Level**, set the value for the level of the entry and above. Specify the **Source** for the entry. Finally, set the **# number of days** that you want to collect event log entries for. If you set this to ***0***, it will go as far back as there is data available.



Event Log Entry

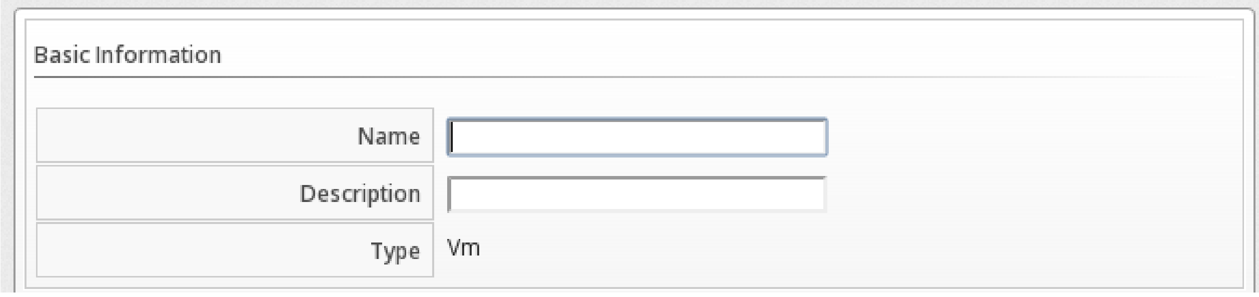
	Name	Filter Message	Level	Source	# of Days
	hostd		warn		5

9. Click **Add**.

5.1.2.3. Creating a Virtual Machine Analysis Profile

Procedure 5.12. To Create a Virtual Machine Analysis Profile

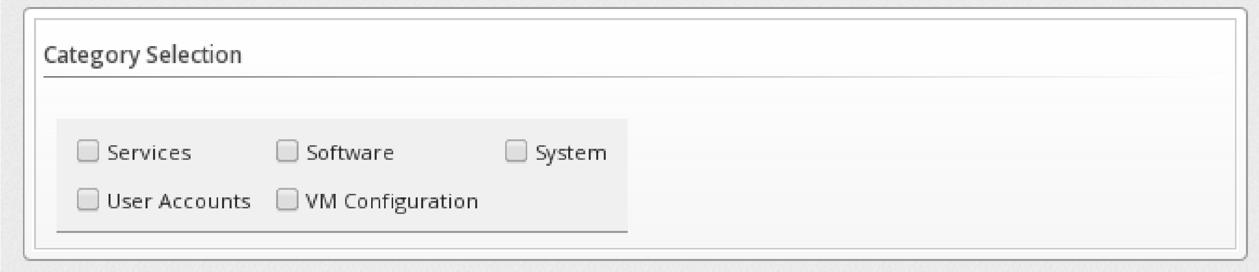
1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Analysis Profiles**.
3. Click ⚙ (**Configuration**), and ➕ (**Add VM Analysis Profile**).
4. In the **Basic Information** area, type in a **Name** and **Description** for the analysis profile.



Basic Information

Name	
Description	
Type	Vm

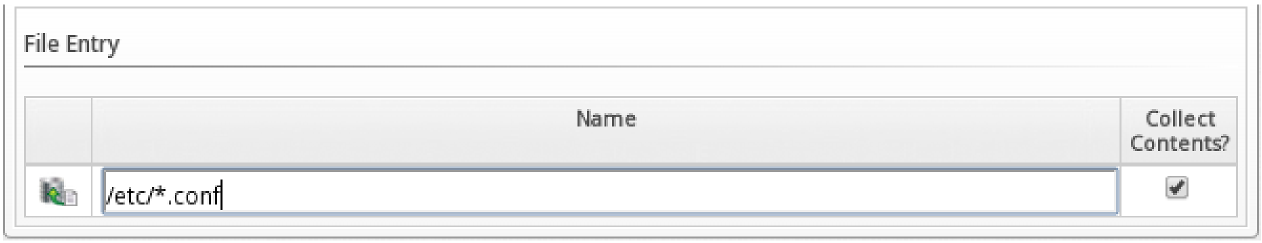
5. You begin in the **Category** area. From the **Category Selection** area, check the categories you want to collect information for. This is available for virtual machine profiles only.



Category Selection

☐ Services ☐ Software ☐ System
☐ User Accounts ☐ VM Configuration

6. Click **File** to collect information about a file or group of files.
7. From the **File Entry** area, type a name, then click ➕ (**Click to add a new entry**) to add a file or group of files. For virtual machines, specify the file to check for. Check the box under **Collect Contents** if you want to collect the file contents as well. The files can be no larger than 1 MB.

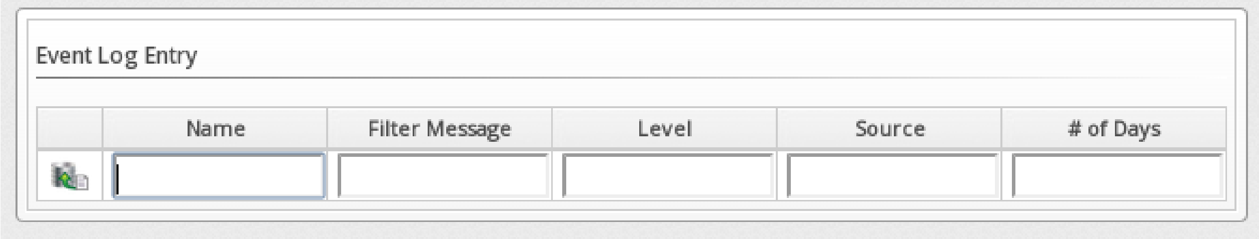


File Entry

	Name	Collect Contents?
	/etc/*.conf	☑

8. Click **Registry** to collect information on a registry key.
9. From the **Registry Entry** area, click ➕ (**Click to add a new entry**) to add a file or group of files. To evaluate whether a registry key exists or does not exist on a virtual machine, without providing a value, type * in the **Registry Value** field. Then, you do not need to know the registry value to collect the keys. This is available for virtual machine profiles only.
10. Click **Event Log** to specify event log entries to collect.

11. From the **Event Log Entry** area, click ✚ (**Click to add a new entry**) to add a type of event log entry. You can type in a specific message to find in **Filter Message**. In **Level**, set the value for the level of the entry and above. Specify the **Source** for the entry. Finally, set the **# (number) of days** that you want to collect event log entries for. If you set this to 0, it will go as far back as there is data available.



Event Log Entry

	Name	Filter Message	Level	Source	# of Days

12. Click **Add**.

5.1.2.4. Editing an Analysis Profile

Procedure 5.13. To Edit an Analysis Profile

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Analysis Profiles**.
3. Check the analysis profile you want to edit.
4. Click ✏ (**Edit this Analysis Profile**).
5. Make any changes.
6. Click **Save**.

Result:

The changes are added to the analysis profile. The virtual machines or hosts must be re-analyzed to collect the new or modified information.

5.1.2.5. Copying an Analysis Profile

Procedure 5.14. To Copy an Analysis Profile

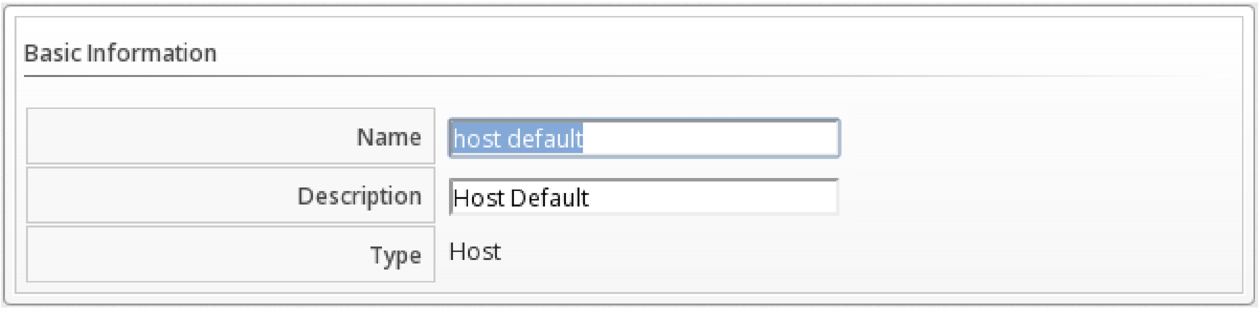
1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Analysis Profiles**.
3. Check the analysis profile you want to copy.
4. Click ⧉ (**Copy this Analysis Profile**).
5. Type a new **Name** and **Description**.
6. Make required changes.
7. Click **Add**.

5.1.2.6. Setting a Default Analysis Profile

If you want to set an analysis profile to be used for all virtual machines, you can create a default profile.

Procedure 5.15. To Create a Default Analysis Profile

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Analysis Profiles**.
3. Click on the analysis profile you want to set as the default.
4. Click ✎ (**Edit this Analysis Profile**).
5. Type **default** for the **Name** for a virtual machine profile. For a host profile, the name should be **host default**.



Basic Information

Name	host default
Description	Host Default
Type	Host

> **Important**
>
> The name must be all lower case.

6. Click **Save**.

5.1.3. Zones

You can organize your CloudForms Management Engine Infrastructure into zones to configure failover and isolate traffic. A provider that is discovered by a server in a specific zone gets monitored and managed in that zone. All jobs, such as a SmartState Analysis or VM power operation, dispatched by a server in a specific zone can get processed by any CloudForms Management Engine Appliance assigned to that same zone.

Zones can be created based on your own environment. You can make zones based on geographic location, network location, or function. When first started, a new server is put into the *default* zone.

Suppose you have four CloudForms Management Engine Appliances with two in the East zone, Appliances A and B, and two in the West zone, Appliances C and D. VC East is discovered by one of the CloudForms Management Engine Appliances in the CloudForms Management Engine Eastern zone. If Appliance A dispatches a job of analyzing twenty virtual machines, this job can be processed by either Appliance A or B, but not C or D.

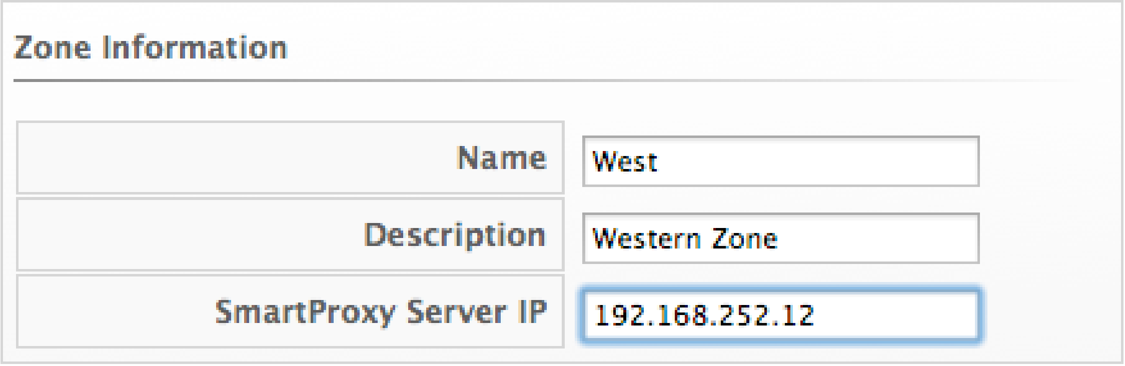
Note

Only users assigned the super administrator role can create zones. There must always be at least one zone. Default zone is provided. This can be removed only after you have created your own zones.

5.1.3.1. Creating a Zone

Procedure 5.16. To Create a Zone

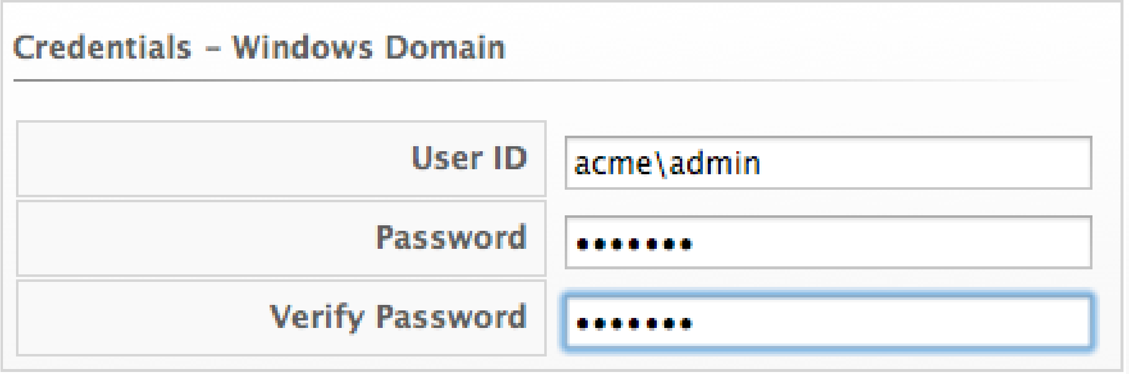
1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click ⚙ (**Configuration**), and ✚ (**Add a new zone**) to create a zone.
4. In the **Zone Information** area, type in a **Name** and **Description** for the new zone.



Zone Information

Name	West
Description	Western Zone
SmartProxy Server IP	192.168.252.12

5. Use **SmartProxy Server IP** to specify the IP address of the server that you want SmartProxies installed in this zone to report to. If this is not set, then the IP address of the server that deployed the SmartProxy is used. This does not apply to embedded SmartProxies.
6. In the **Credentials - Windows Domain** area, type in Windows domain credentials to be able to collect running processes from Windows virtual machines that are on a domain.



Credentials – Windows Domain

User ID	acme\admin
Password	•••••••
Verify Password	•••••••

7. Optionally, you can configure NTP servers for the entire zone in the **NTP Servers** area. These settings will be used if the NTP servers have not been set for the appliance in the Operations-Server page.

8. In the **Settings** area, set the number for **Max Active VM Scans**. The default is **Unlimited**.

9. Click **Save**.

5.1.3.2. Deleting a Zone

Procedure 5.17. To Delete a Zone

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone you want to remove.

> **Note**
>
> You cannot delete a zone if there are servers assigned to it.

4. Click ⚙ (**Configuration**), then click 🗑 (**Delete this Zone**).
5. Click **OK** to confirm.

5.1.3.3. Editing a Zone

Procedure 5.18. To Edit a Zone

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone you want to edit.
4. Click ⚙ (**Configuration**), then click ✏ (**Edit this Zone**).
5. Make the required changes.
6. Click **Save**.

5.1.3.4. SmartProxy Affinity

If you are using embedded SmartProxies, you can select which hosts they are allowed to analyze. Embedded SmartProxies are those that are run as a role from a server. This helps to control or eliminate unnecessary network traffic. Recall that a server is using the embedded SmartProxy if its SmartProxy server role is enabled.

5.1.3.4.1. Assigning Embedded SmartProxies to Hosts

Procedure 5.19. To Assign Embedded SmartProxies to Hosts

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.

3. Click the zone you want to edit.

4. Click the **SmartProxy Affinity** tab.

5. If you have multiple servers in the selected zone, select the one you want to configure from the **Server** dropdown in the **Assign Hosts to Embedded SmartProxies** area. If there is only one server with the SmartProxy role enabled, you cannot select a specific server. If there are no embedded SmartProxies being used in that zone, you cannot select any servers.

6. Select the hosts you want to assign to this embedded SmartProxy from **Available Hosts**.

7. Click ▶ (**Move selected Hosts right**).

8. Click **Save**.

5.1.4. Servers

Server settings enables you to control how each CloudForms Management Engine server operates including authentication, logging, and email. If you have multiple servers in your environment that are reporting to one central VMDB, then you can edit some of these settings from the console by specifying which server you want to change.

> **Note**
>
> The server selection options are only available if you have multiple servers sharing one VMDB.

5.1.4.1. Changing Server Settings

Procedure 5.20. To Change Server Settings

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Settings** accordion, then click **Zones**.

3. Click the zone where the CloudForms Management Engine server is located.

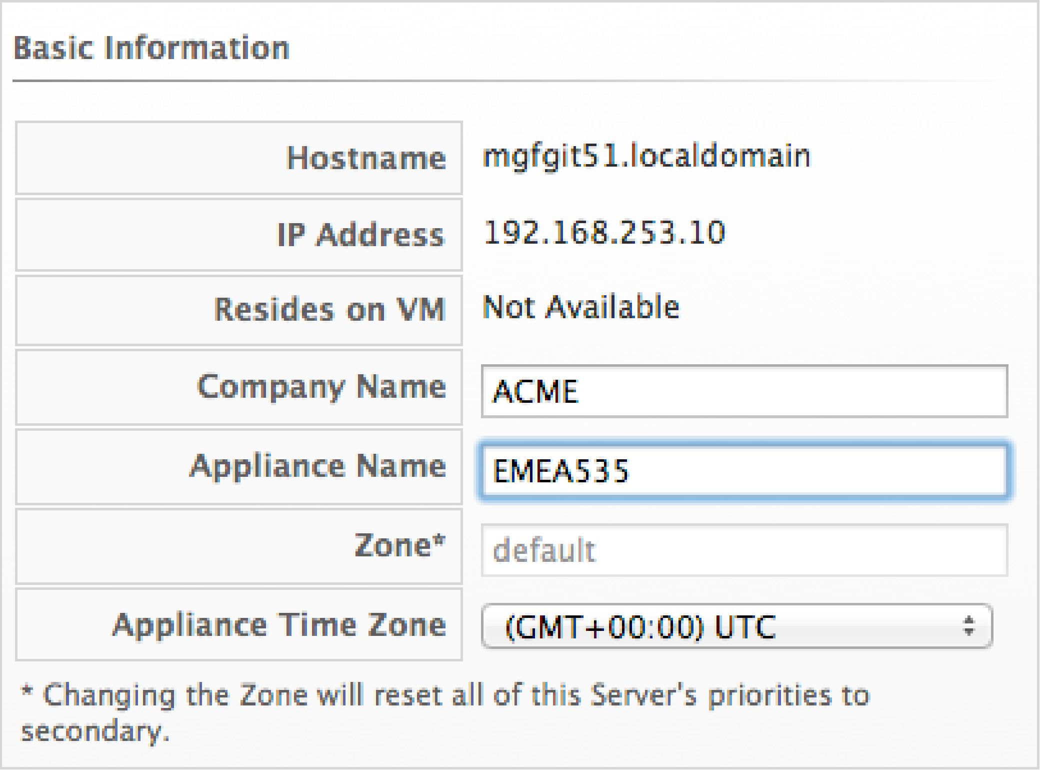
4. In the **Servers** area, click on the CloudForms Management Engine server.

5. Click **Server**.

6. Make any required changes.

7. Click **Save**.

5.1.4.1.1. Basic Information Settings



Basic Information

Hostname	mgfgit51.localdomain
IP Address	192.168.253.10
Resides on VM	Not Available
Company Name	ACME
Appliance Name	EMEA535
Zone*	default
Appliance Time Zone	(GMT+00:00) UTC

* Changing the Zone will reset all of this Server's priorities to secondary.

- Use **Company Name** (maximum 20 characters) to customize the interface with your company's name. You will see the company name when you are viewing or modifying the tags of an infrastructure object or virtual machine.
- Specify the **Appliance Name** (maximum 20 characters) you want displayed as the appliance that you are logged into. You will see this in the upper right corner of the interface with the name of the consoles logged on user.
- Use **Zone** to isolate traffic and provide load balancing capabilities. Specify the zone that you want this CloudForms Management Engine Appliance to be a member of. At startup, the zone is set to default.
- Use **Appliance Time Zone** to set the time zone for this server.

Note

This is the time zone used when created scheduled analyses. This is not the same as the **Time Zone** parameter, which is found by navigating to **Configure** → **My Settings**, then exploring the **Display Settings** area, and is the time zone displayed in the console.

5.1.4.1.2. Server Control Settings

Server role defines what a server can do. Red Hat recommends that **Database Operations**, **Event Monitor**, **Reporting**, **Scheduler**, **SmartState Analysis**, **User Interface**, **Provider Inventory**, **Provider Operations**, and **Web Services** be enabled on at least one server in each zone. These roles are enabled by default on all servers.

- Use **Default Repository SmartProxy** to set the SmartProxy from which you will be refreshing your virtual machine repositories. This host must have access to your repositories to analyze its virtual machines.

Note

- Only super administrators can change server roles.
- If you are using more than one CloudForms Management Engine Appliance, be sure to set this on all of the appliances.

5.1.4.1.3. Server Roles

Server Role	Description
Automation Engine	Use this role if you want to use this CloudForms Management Engine server to process automation tasks.
Capacity and Utilization (3 Server Roles)	- The **Capacity & Utilization Coordinator** role checks to see if it is time to collect data, somewhat like a scheduler. If it is time, a job is queued for the Capacity and Utilization Data Collector. The coordinator role is required to complete Capacity and Utilization data collection. If more than one CloudForms Management Engine server in a specific zone has this role, only one will be active at a time. - The **Capacity & Utilization Data Collector** performs the actual collection of capacity and utilization data. This role has a dedicated worker, and there can be more than one CloudForms Management Engine server with this role in a zone. - The **Capacity & Utilization Data Processor** processes all of the data collected, allowing CloudForms Management Engine to create charts. This role has a dedicated worker, and there can be more than one CloudForms Management Engine server with this role in a zone.
Database Operations	Use Database Operations to enable this CloudForms Management Engine server to run database backups or garbage collection.
Database Synchronization	Use **Database Synchronization** to enable this CloudForms Management Engine server's VMDB to replicate to a higher-level VMDB. This should only be enabled after creating settings for the Replication Worker.

Server Role	Description
Event Monitor	This role is enabled by default and provides the information shown in timelines. **`Event Monitor`** is responsible for the work between the CloudForms Management Engine server and your providers. It starts 2 workers for each provider. One worker, the monitor, is responsible for maintaining a connection to a provider, catching events, and putting them on the CloudForms Management Engine message queue for processing. The second worker, the handler, is a message queue worker responsible for delivering only those messages for a provider. You should have at least one of these in each zone.
Provider Inventory	This role is enabled by default. This role is responsible for refreshing provider information including EMS, hosts, virtual machines, and clusters, and is also responsible for capturing datastore file lists. If more than one CloudForms Management Engine server in a specific zone has this role, only one will be active at a time.
Provider Operations	This role is enabled by default. This role sends stop, start, suspend, shutdown guest, clone, reconfigure, and unregister to the provider, directly from the console or through a policy action if you have CloudForms Management Engine Control. More than one CloudForms Management Engine server can have this role in a zone.
Notifier	Use this role if you will be using CloudForms Management Engine Control or Automate to forward SNMP traps to a monitoring system or send e-mails. See the *CloudForms Management Engine Control Guide* for details on creating SNMP alerts. If more than one CloudForms Management Engine server in a specific zone has this role, only one will be active at a time.
Reporting	This role is enabled by default. The **`Reporting`** role specifies which CloudForms Management Engine servers can generate reports. If you do not have a CloudForms Management Engine server set to this role in a zone, then no reports can be generated in that zone. You should have at least one of these in each zone.

Server Role	Description
RHN Mirror	An appliance with **RHN Mirror** enabled acts as a server containing a repository with the latest CloudForms Management Engine packages. This also configures other Appliances within the same region to point to the chosen **RHN Mirror** server for updates. This provides a low bandwidth method to update environments with multiple Appliances.
Scheduler	This role is enabled by default. The **Scheduler** sends messages to start all scheduled activities such as report generation and SmartState Analysis. This role also controls all system schedules such as capacity and utilization data gathering. One server in each zone must be assigned this role or scheduled CloudForms Management Engine events will not occur. If more than one CloudForms Management Engine server in a specific zone has this role, only one will be active at a time.
SmartProxy	Enabling the **SmartProxy** role turns on the embedded SmartProxy on the CloudForms Management Engine server. The embedded SmartProxy can analyze virtual machines that are registered to a Host and templates that are associated with a provider. To provide visibility to repositories, install the SmartProxy on a host from the CloudForms Management Engine console. This SmartProxy can also analyze virtual machines on the host on which it is installed.
SmartState Analysis	This role is enabled by default. The **SmartState Analysis** role controls which CloudForms Management Engine servers can control SmartState Analyses and process the data from the analysis. You should have at least one of these in each zone.
User Interface	This role is enabled by default. Uncheck **User Interface** if you do *not* want users to be able to access this CloudForms Management Engine server using the CloudForms Management Engine console. For example, you may want to turn this off if the CloudForms Management Engine server is strictly being used for capacity and utilization or reporting generation. More than one CloudForms Management Engine server can have this role in a zone.

Server Role	Description
Web Services	This role is enabled by default. Uncheck **Web Services** to stop this CloudForms Management Engine server from acting as a Web service provider. More than one CloudForms Management Engine server can have this role in a zone.

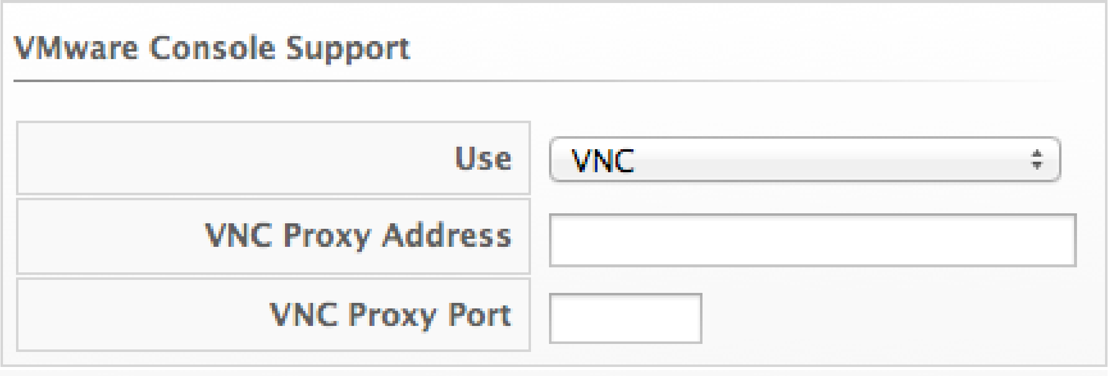
5.1.4.1.4. VMware Console Settings

If you are using the CloudForms Management Engine Control feature set, then you have the ability to connect to a Web console for virtual machines that are registered to a host. To use this feature, you must have VNC installed, the appropriate version of the VMware MKS plug-in or the appropriate VMRC viewer installed in your Web browser. Note that you are responsible for installing the correct version for your virtual infrastructure. See the vendors documentation for information.

After installing the appropriate software or version, you must specify which version you are using in the CloudForms Management Engine configuration settings.

Note

To edit the **VMware MKS plug-in** settings, you must have the super administrator role.



VMware Console Support

Use	VNC
VNC Proxy Address	
VNC Proxy Port	

- If you select **VNC**, type in the port number used. This port must be open on the target virtual machine and the VNC software must be installed there. On the computer that you are running the console from, you must install the appropriate version of **Java Runtime** if it is not already installed.
- If you select **VMware MKS plug-in**, select the appropriate version.
- If using **VMware VMRC plug-in**, be sure that you have fulfilled the requirements.

  The correct version of the VMRC plug-in from VMware must be installed on the client computer. To do this, log into the Virtual Center Web Service and attempt to open a virtual machine console. This should prompt you to install the required plug-in.

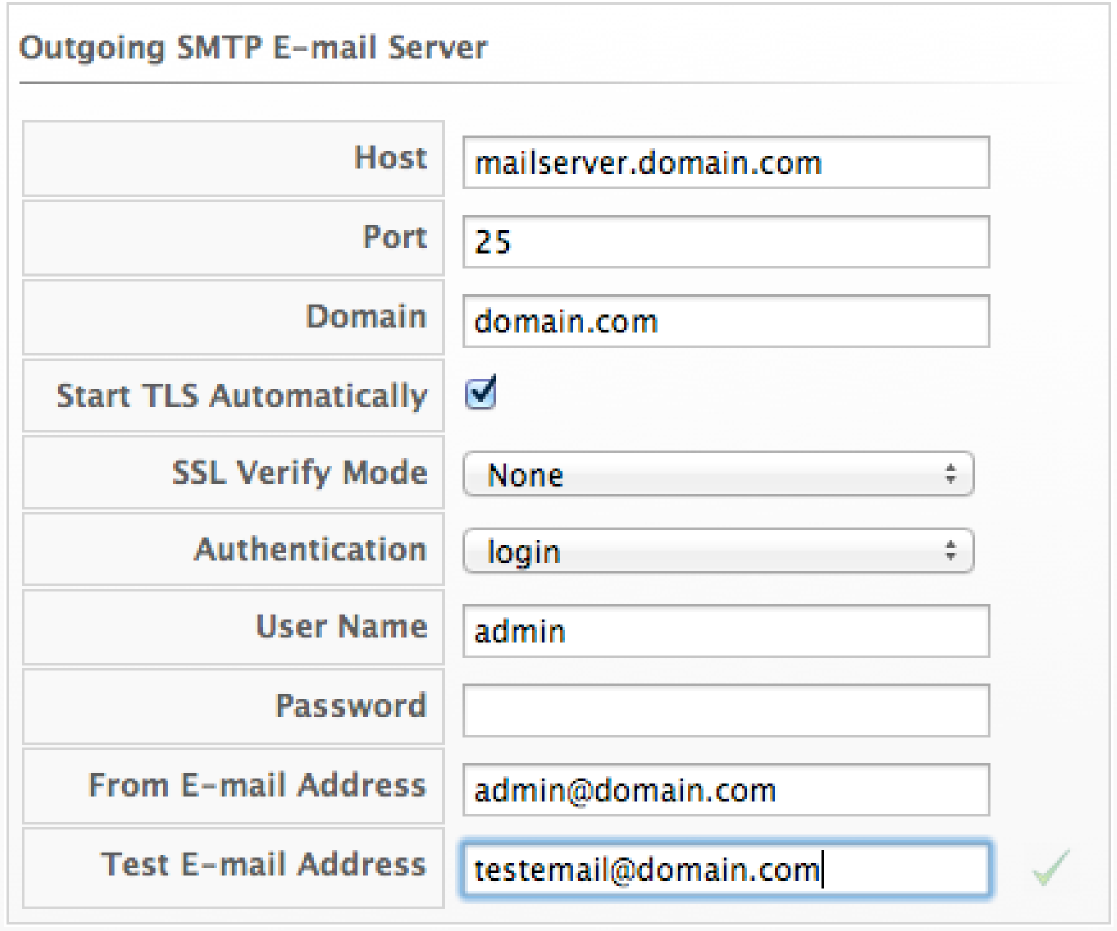
  The VSphere Web Client must be installed on VC version 5, and the provider must be registered to it. For Virtual Center version 4, the VMware VirtualCenter Management Webservice must be running.

5.1.4.1.5. Outgoing SMTP Email Settings

To use the email action in CloudForms Management Engine, set an email address that you will have the emails sent from.

Note

To be able to send any emails from the server, you must have the **Notifier** server role enabled. You can test the settings without the role enabled.



Outgoing SMTP E-mail Server

Host	mailserver.domain.com
Port	25
Domain	domain.com
Start TLS Automatically	☑
SSL Verify Mode	None
Authentication	login
User Name	admin
Password	
From E-mail Address	admin@domain.com
Test E-mail Address	testemail@domain.com ✓

- Use **Host** to specify the host name of the mail server.
- Use **Port** to specify the port for the mail server.
- Use **Domain** to specify domain name for the mail server.
- Check **Start TLS Automatically** if the mail server requires TLS.
- Select the appropriate **SSL Verify Mode**.
- Use the **Authentication** drop down to specify if you want to use login or plain authentication.
- Use **User Name** to specify the user name required for login authentication.
- Use **Password** to specify the password for login authentication.
- Use **From Email Address** to set the address you want to send the email from.
- Use **To Email Address** if you want to test your email settings.

5.1.4.1.5.1. Testing Outgoing SMTP Email Server Settings

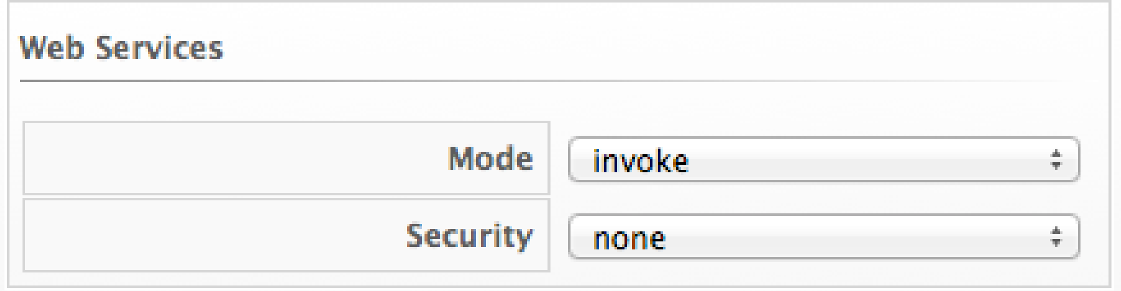
Procedure 5.21. To Test Outgoing SMTP Email Server Settings

1. Type in all settings in the Outgoing SMTP Email Server settings, including **`Test Email Address`**.

2. Click ✓ (**`Send test email`**).

5.1.4.1.6. Web Services Settings

Web services are used by the server to communicate with the SmartProxy.



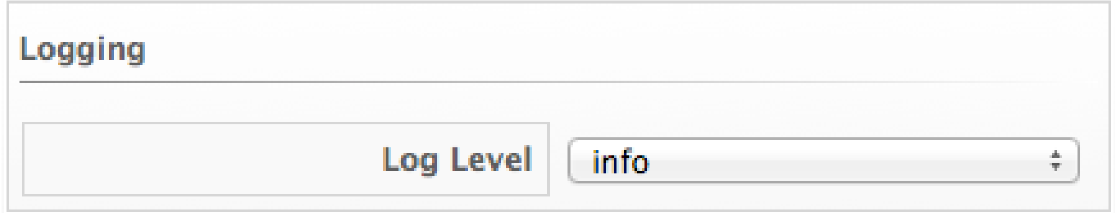
Web Services

Mode	invoke
Security	none

- Set **`Mode`** to invoke to enable 2-way Web services communication between the CloudForms Management Engine Appliance and the SmartProxy. Set **`Mode`** to disabled to use Web services from the SmartProxy to the CloudForms Management Engine Appliance only. When the CloudForms Management Engine Appliance has work for the SmartProxy, the work will be placed in a queue in the VMDB. The work will be completed either when the CloudForms Management Engine Appliance is able to contact the SmartProxy or when the next SmartProxy heartbeat occurs, whichever comes first.

- If Web services are enabled, you have the option to use **`ws-security`**.

5.1.4.1.7. Logging Settings

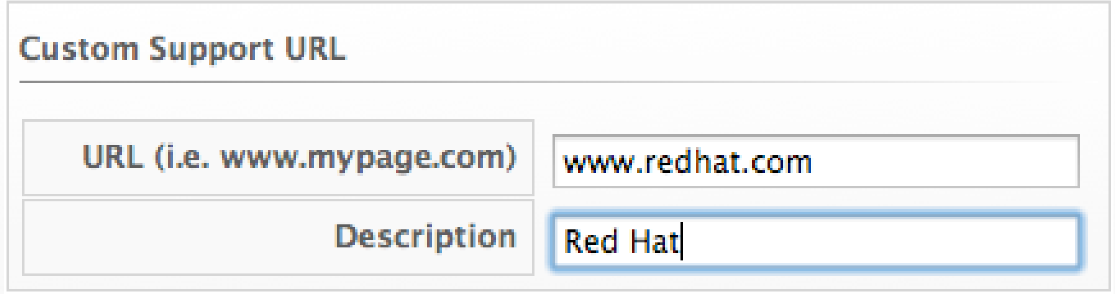


Logging

Log Level	info

- Use **`Log Level`** to set the level of detail you want in the log. You can select from fatal, error, warn, info, and debug. The default setting is 'info'.

5.1.4.1.8. Custom Support URL Settings



Custom Support URL

URL (i.e. www.mypage.com)	www.redhat.com
Description	Red Hat

- Use **URL** to specify a specific URL that you want to be accessible from the **About Product Assistance** area.

- Use **Description** to set a label for the URL.

5.1.4.2. Authentication

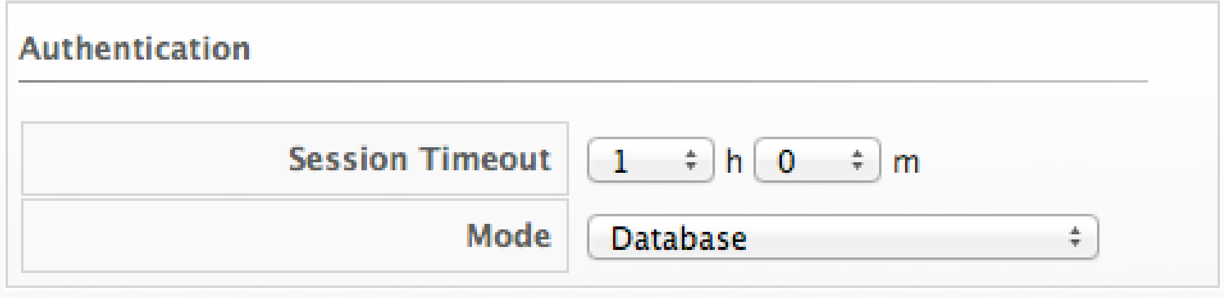
Use the **Authentication** tab to specify how you want users authenticated on the console. You can use the VMDB or integrate with LDAP, LDAPS, or Amazon.

5.1.4.2.1. Changing an Authentication Setting

Procedure 5.22. To Change an Authentication Setting

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone where the server is located.
4. Click on the server.
5. Click on the **Authentication** tab.
6. Make any required changes. If you check **LDAP**, **LDAPS**, or **Amazon** as the authentication mode, click **Validate** to check your settings in the **Role Settings** area.
7. Click **Save**.

5.1.4.2.2. Authentication Settings



Authentication

Session Timeout 1 h 0 m

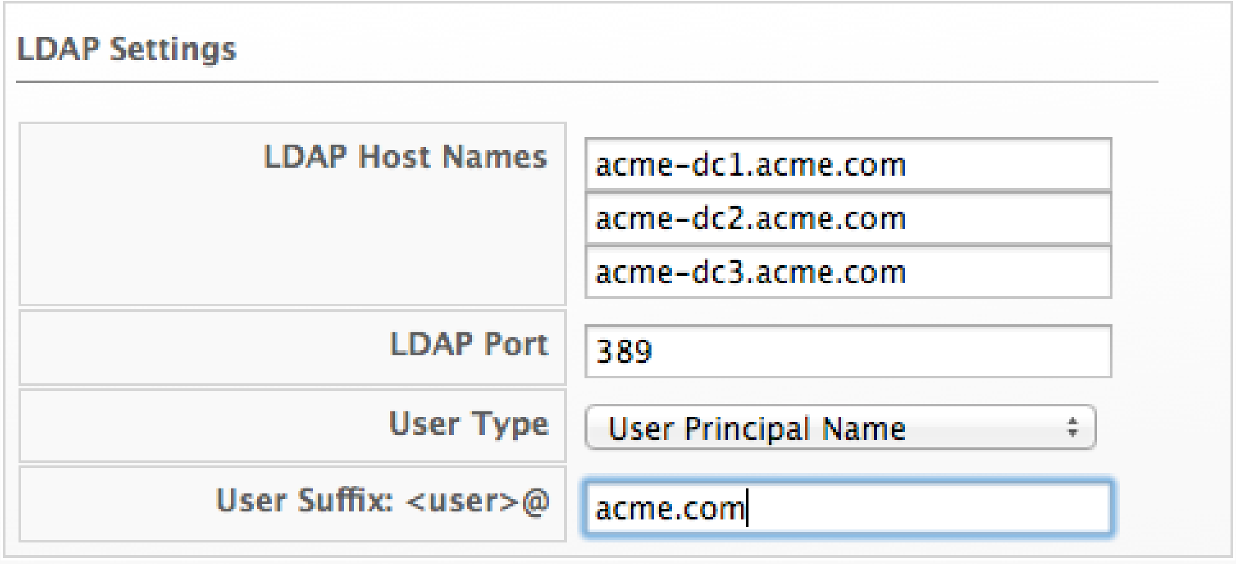
Mode Database

- Use **Session Timeout** to set the period of inactivity before a user is logged out of the console.

- Use **Mode** to set the type of authentication. Choose from **Database** (using the VMDB), **LDAP** (Lightweight Directory Authentication Protocol), **LDAPS** (Secure Lightweight Directory Authentication Protocol), or **Amazon**. The default is **Database**. If you choose **Database**, see *Creating a User* to create users. See *LDAP Settings* for more information on configuration for LDAP and LDAPS. If you choose **Amazon**, see *Amazon Settings*.

5.1.4.2.3. LDAP Settings

If you choose LDAP or LDAPS as your authentication mode, required parameters are exposed under LDAP Settings. Be sure to validate your setting before saving them.


LDAP Settings

LDAP Host Names	acme-dc1.acme.com acme-dc2.acme.com acme-dc3.acme.com
LDAP Port	389
User Type	User Principal Name
User Suffix: <user>@	acme.com

- Use **LDAP Host Name** to specify the fully qualified domain names of your LDAP servers. CloudForms Management Engine will search each host name in order until it finds one that authenticates the user.

- Use **LDAP Port** to specify the port for your LDAP server. The default is 389 for LDAP and 636 for LDAPS.

- From the **User Type** dropdown select **User Principal Name** to type the user name in the format of user@domainname. Select Email Address to login with the users email address. Select Distinguished Name (CN=<user>) or Distinguished Name (UID=<user>) to use just the user name, but be sure to enter the proper **User Suffix** for either one. Choose the correct Distinguished Name option for your directory service implementation.

- Specify the **User Suffix**, such as *acme.com* for **User Principal Name** or *cn=users,dc=acme,dc=com*for Distinguished Name, in Base DN.

5.1.4.2.4. Amazon Settings

If you choose Amazon as your authentication mode, required parameters are exposed under **Amazon Primary AWS Account Settings for IAM**. Be sure to validate your setting before saving them.

- Type in an **Access Key** provided by your Amazon account.

- Type in a **Secret Key** provided by your Amazon account.

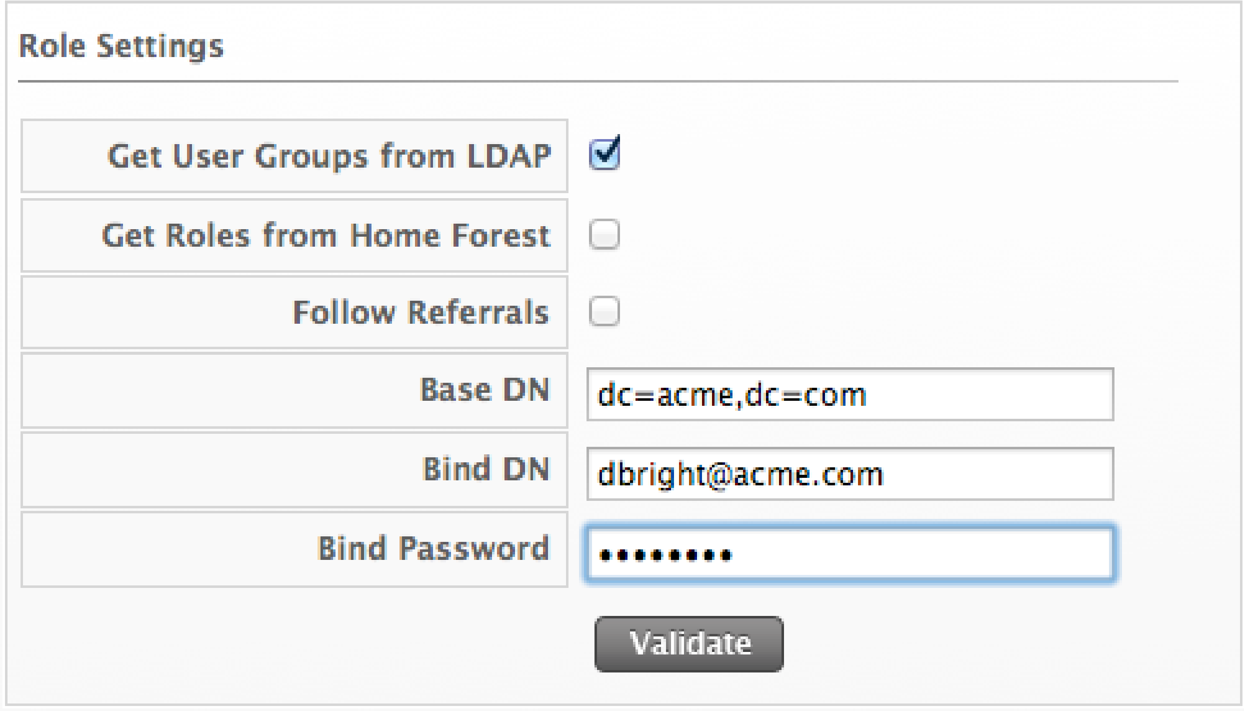
Users logging into CloudForms Management Engine with Amazon authentication enter their own **IAM Access Key** as the username and **IAM Secret Key** as the password. Amazon users must be added as a CloudForms Management Engine user or belong to an IAM user group added to the list of CloudForms Management Engine groups.

5.1.4.2.5. Role Settings

If you choose LDAP, you can use groups from your directory service to set the role for the authenticated LDAP User. The LDAP user must be in one of the Account Role Groups. See LDAP Groups.

If you do not check **Get User Groups from LDAP**, the user must be defined in the VMDB using the console where the User ID is the same as the user's name in your directory service typed in lowercase. For example, **dbright@acme.com** when using User Principal

Name, **cn=dan bright,ou=users,dc=acme,dc=com** when using Distinguished Name (**CN=<user>**), or **uid=dan bright,ou=users,dc=acme,dc=com** when using Distinguished Name (**UID=<user>**). Then, when logging in, the user would type either **dbright** (User Principal Name) or **dan bright** (Distinguished Name). If the user is not defined in the VMDB, they will be denied access to CloudForms Management Engine.



Role Settings

Get User Groups from LDAP	☑
Get Roles from Home Forest	☐
Follow Referrals	☐
Base DN	dc=acme,dc=com
Bind DN	dbright@acme.com
Bind Password	••••••••

- Check **Get Roles from Home Forest** to use the LDAP roles from the LDAP users home forest.
- Check **Follow Referrals** to lookup and bind a user that exists in a domain other than the one configured in the LDAP authentication settings.
- Use **Base DN** to set the place in the directory tree from which you want to start searching for users.
- Specify the user name to bind to the LDAP server in **Bind DN**. This user must have read access to all users and groups that will be used for CloudForms Management Engine authentication and role assignment.
- Specify the password for the Bind DN user in **Bind Password**.

Click **Validate** to verify your settings.

5.1.4.2.6. Trusted Forests

5.1.4.2.6.1. Trusted Forest Settings

If a user has group memberships in another LDAP Forest, then specify the settings to access the memberships in the trusted forest.

5.1.4.2.6.2. Adding Settings for a Trusted Forest

Procedure 5.23. To Add Settings for a Trusted Forest

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.

3. Click the Zone where the Server is located.

4. Click on the Server.

5. Click Authentication.

6. Check Get Role from LDAP, and enter all items in the Role Settings Area.

7. In the Trusted Forest Settings area, click + (**`Click to add a new forest`**).

8. Enter the LDAP Host Name, select a Mode, and enter an LDAP Port, Base DN, Bind DN, and Bind Password.

9. Click Save.

5.1.4.3. Workers

Use the Workers page to specify the number of workers and amount of memory allowed to be used for each type.

Note

Only make these changes when directed to by Red Hat Support.

5.1.4.3.1. Changing Settings for a Worker

Procedure 5.24. To Change the Settings for a Worker (except replication worker)

1. Navigate to **Configure** → **Configuration**.

2. Click on the **`Settings`** accordion, then click **`Zones`**.

3. Click the zone where the server is located.

4. Click on the server.

5. Click **`Workers`**.

6. Go to the type of worker you have been directed to change.

7. If applicable, change **`Count`** or **`Memory Threshold`** using the dropdown boxes.

8. Click **`Save`**.

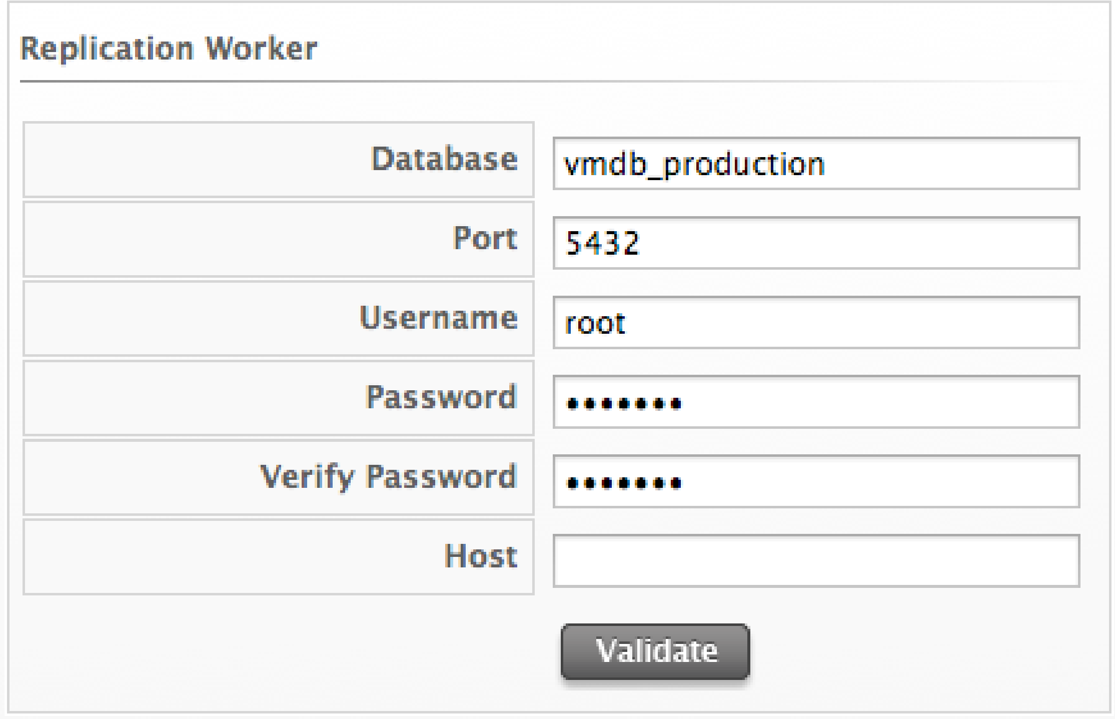
5.1.4.3.2. Changing Settings for the Replication Worker

Important

This should only be entered on subordinate servers that will have the Database Synchronization role enabled. These settings must be completed before enabling that role.

Procedure 5.25. To Change Settings for the Replication Worker

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone where the server is located.
4. Click on the server.
5. Click **Workers**.
6. Go to the **Replication Worker** area.



Replication Worker

Database	vmdb_production
Port	5432
Username	root
Password	•••••••
Verify Password	•••••••
Host	

- Use **Database** to specify the name of your VMDB.
- Specify the **User Name** to connect to the VMDB.
- Use **Password** and **Verify Password** to specify the password for the user name.
- Use **Host** to specify the IP address or hostname of the top level VMDB.

7. Click **Validate** to confirm that the VMDB is accessible.
8. Click **Save**.

Result:

The new settings take one to two minutes to take effect. Next, you need to enable the replication worker on the subordinate regions VMDB server.

5.1.4.4. Database

Use the Database page to specify the location of your Virtual Machine Database (VMDB) and its login credentials. By default, the type is PostgreSQL on the Server.

Note

The server may not start if the database settings are changed. Be sure to validate your new settings before restarting the server.

5.1.4.4.1. Changing a Database Setting

Procedure 5.26. To Change a Database Setting

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone where the server is located.
4. Click on the server.
5. Click the **Database** tab.
6. In the **Database** area, select the **Type** of database. You can select from **External Database on another Server**, **External PostgreSQL Database**, and **Internal Database on this Appliance (default)**. The rest of the possible settings will vary depending on which type of database you chose.
   - Use **Hostname** to specify the IP address or hostname of the external database server.
   - Use **Database Name** to specify the name of your VMDB.
   - Specify the **User Name** to connect to the VMDB.
   - Use **Password** and **Verify Password** to specify the password for the user name.
7. Click **Validate** to check the settings.
8. Click **Save**.
9. Click **OK** to the warning that the server will restart immediately after you save the changes.

Result:

During the restart, you are unable to access the server. When the restart is complete, the new database settings are in effect.

5.1.4.5. Customization and Logos

5.1.4.5.1. Custom Logos

Use **Custom Logos** to display your own logo in the corner of the console or on the CloudForms Management Engine login panel.

5.1.4.5.2. Uploading a Custom Logo to the Console

Procedure 5.27. To Upload a Custom Logo to the Console

1. Make sure the desired logo is accessible from the computer where you are running the console. The file must be in portable network graphics (png) format with dimensions of 350 x 70.

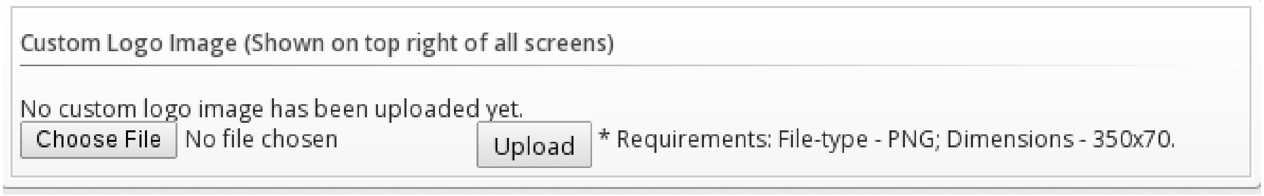
2. Navigate to **Configure** → **Configuration**.

3. Click on the **Settings** accordion, then click **Zones**.

4. Click the zone where the CloudForms Management Engine server is located.

5. Click on the server.

6. Click the **Custom Logos** tab.



No custom logo image has been uploaded yet.

* Requirements: File-type - PNG; Dimensions - 350x70.

7. Click **Choose File** in the **Custom Logo Image (Shown on top right of all screens)** area to go to the location where the logo file is located.

8. Click **Upload**. The icon is displayed above the file name box, and an option is shown to use the logo.

9. Check **Use Custom Logo Image** to add the logo to your console.

10. Click **Save**.

5.1.4.5.3. Customizing the Login Panel

Procedure 5.28. To Customize the Login Panel

1. Make sure the logo that you want to use is accessible from the computer where you are running the console. The file must be in a PNG format with dimensions of 1280 x 1000.

2. Navigate to **Configure** → **Configuration**.

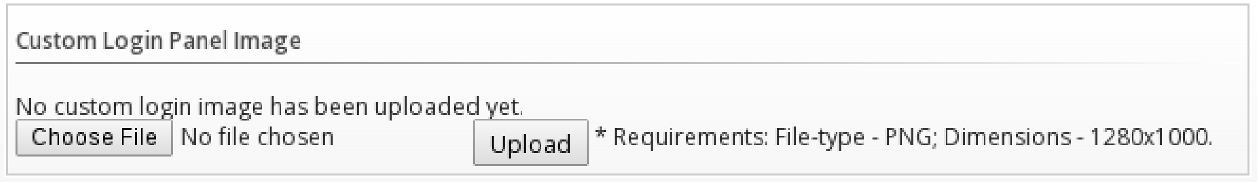
3. Click on the **Settings** accordion, then click **Zones**.

4. Click the zone where the server is located.

5. Click on the server.

6. Click the **Custom Logos** tab.

7. Click **Choose File** in the **Custom Login Panel Image** area to go to the location where the logo file is located.



No custom login image has been uploaded yet.

* Requirements: File-type - PNG; Dimensions - 1280x1000.

8. Click **Upload**. The icon is displayed above the file name box, and an option is shown to use the logo.

9. Check Use **Custom Login Image** to add the logo to your console.

10. Click **Save**.

5.1.4.5.4. Customizing the Login Panel Text

Procedure 5.29. To Customize the Login Panel Text

1. Navigate to **Configure** → **Configuration**.

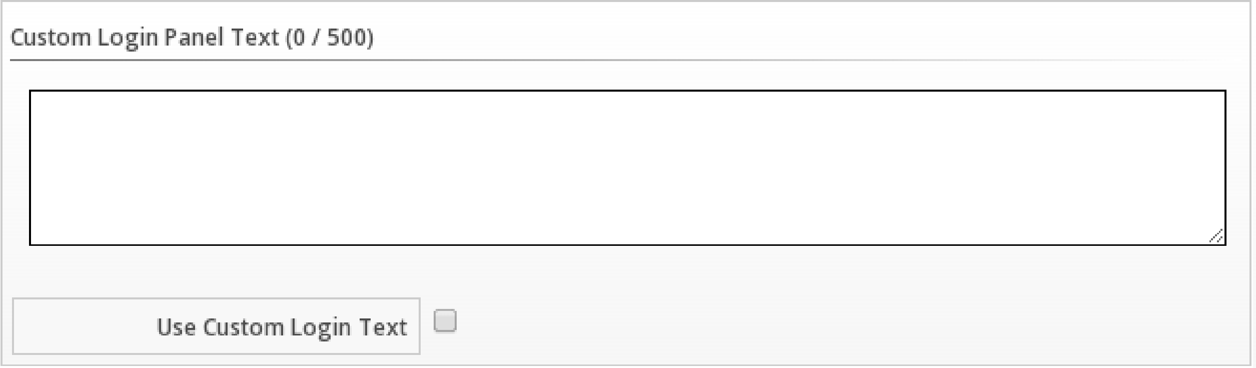
2. Click on the **Settings** accordion, then click **Zones**.

3. Click the zone where the server is located.

4. Click on the server.

5. Click the **Custom Logos** tab.

6. In **Custom Login Panel Text**, type in text that you want to show on the consoles login screen.


Custom Login Panel Text (0 / 500)

Use Custom Login Text □

7. Check **Use Custom Login Text** box to add the text to the screen.

8. Click **Save**.

5.1.4.6. SmartProxy

Use these settings to configure default behaviors of your host-based SmartProxies such as frequency of heartbeats, ports, and log settings.

> **Note**
>
> These settings are only for SmartProxies installed from this point forward. To change the settings for an already installed SmartProxy, see Editing the SmartProxy Settings.

5.1.4.6.1. Changing Host Based SmartProxy Default Settings

Procedure 5.30. To Change Host Based SmartProxy Default Settings

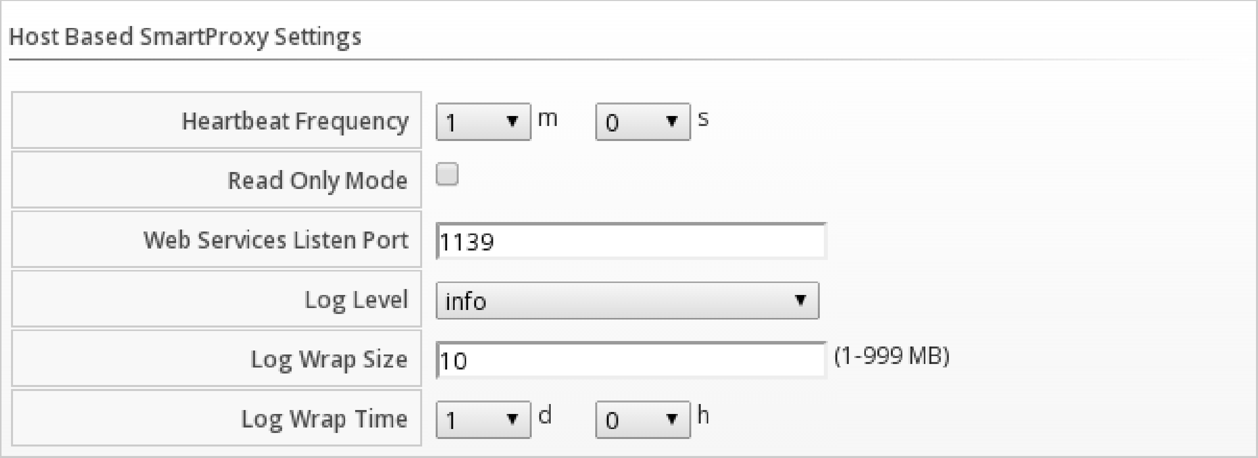
1. Navigate to **Configure** → **Configuration**.

2. Click on the **Settings** accordion, then click **Zones**.

3. Click the zone where the server is located.

4. Click on the server.

5. Click the **SmartProxy** tab.



Host Based SmartProxy Settings

Heartbeat Frequency	1 ▾ m 0 ▾ s
Read Only Mode	□
Web Services Listen Port	1139
Log Level	info ▾
Log Wrap Size	10 (1-999 MB)
Log Wrap Time	1 ▾ d 0 ▾ h

- Use **Heartbeat Frequency** to configure how often you want the SmartProxy to contact the server to check for tasks.

- Check **Read Only Mode** so that the SmartProxy will not perform any tasks that change the host computer or virtual machines. For example, the SmartProxy will discover and analyze, but will not stop, start, or pause virtual machines.

- Use **Web Services Listen Port** to specify the port you want web services for the SmartProxy to listen on. The default is port 1139.

- Use **Log Level** to specify the default log level for the SmartProxys log.

- Use **Log Wrap Size** to set a size for the log to wrap in megabytes. The size can be from 1 to 999 MB.

- Use **Log Wrap Time** to set a time frequency for log wrapping. The units are in days and hours.

> **Note**
>
> The log wrapping will occur on whichever limit is reached first, size or time.

6. Click **Save**.

5.1.4.7. Advanced Settings

5.1.4.7.1. Advanced

You may be instructed by Red Hat to edit some configuration settings manually. This feature is available for a limited number of options and can only be used by users assigned the super administrator role. Changing settings using this procedure may disable your CloudForms Management Engine server.

Note

Only make manual changes to your configuration files if directed to do so by Red Hat.

5.1.4.7.2. Editing Configuration Files Manually

Procedure 5.31. To Edit Configuration Files Manually

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone where the server is located.
4. Click on the server.
5. Click the **Advanced** tab.
6. Select the configuration file to edit from the **Configuration File to Edit** area.
7. Make the required changes.
8. Click **Save**.

5.1.4.7.3. Configuration Parameters

Table 5.1. authentication

Parameters	Description
amazon_key	If using Amazon for the authentication mode, specify your Amazon Key. This is the same as Amazon Access Key in Configuration-Operations- Server-Amazon Settings in the CFME Console. Default: blank
amazon_secret	If using Amazon for the authentication mode, specify your Amazon Secret. This is the same as Amazon Secret Key in Configuration-Operations- Server-Amazon Settings in the CFME Console. Default: blank
basedn	If using ldap for the authentication mode, specify your Base DN. This is the same as Base DN in Configuration-Operations- Server-LDAP Settings in the CFME Console. Default: blank

Parameters	Description
bind_dn	The user name to bind to the LDAP server. This user must have read access to all users and groups that will be used for CFME authentication and role assignment. This is the same as Bind DN in Configuration-Operations- Server-LDAP Settings in the CFME Console. Default: blank
bind_pwd:	The password for the bind_dn user. This is the same as Bind Password in Configuration-Operations-Server-LDAP Settings in the CFME Console. Default: blank
get_direct_groups	Use this to get the LDAP roles from the LDAP users' home forest. This is the same as Get Roles from Home Forest in the **`Authentication`** page for the CFME Server. Default: true
group_memberships_max_depth	When traversing group memberships in the LDAP directory it will stop at this value. Default: 2
ldaphost	Use ldaphost to specify the fully qualified domain name of your LDAP server. This is the same as LDAP Host Name in Configuration-Operations-Server-LDAP Settings in the CFME Console. Default: blank
ldapport	Specify the port of your LDAP server. This is the same as LDAP Port in Configuration-Operations-Server-LDAP Settings in the CFME Console. Default: 389
mode	Use database to use the VMDB for security. Use ldap or ldaps to use directory services. This is the same as Mode in Configuration-Operations- Server-Authentication in the CFME Console. Default: database

Parameters	Description
user_type	Use userprincipalname to type the user name in the format of *user@domainname*. Use mail to login with the user's e-mail address. Use dn-cn for Distinguished Name (CN=<user>) or dn-uid Distinguished Name (UID=<user>) to use just the user name, but be sure to enter the proper user_suffix for either one. This is the same as User Type in Configuration-Operations- Server-LDAP Settings in the CFME Console. Default: userprincipalname
user_suffix	Domain name to be used with user_type of dn-cn or dn-uid. This is the same as User Suffix in Configuration-Operations- Server-LDAP Settings in the CFME Console. Default: blank

Table 5.2. coresident_miqproxy

Parameters	Description
use_vim_broker	Specify if you want the coresident SmartProxy to use a shared connection through the VIM broker to communicate with the VC or ESX host for SmartState Analysis. If it is disabled, then each SmartProxy SmartState Analysis would create its own connection. Default: true
concurrent_per_ems	Specify the number of co-resident SmartProxy SmartState Analyses that can be run against a specific management system at the same time. Default: 1
concurrent_per_host	Specify the number of co-resident SmartProxy SmartState Analyses that can be run against a specific host at the same time. Default: 1
scan_via_host	If you change scan_via_host to false, CFME will use the Management System to scan which is limited by the concurrent_per_ems setting instead of the concurrent_per_host setting. Note this will greatly increase traffic to the Management System. Default: true

Table 5.3. ems_refresh

Parameter	Description
capture_vm_created_on_date	Set to false to turn off historical event retrieval. Set to true to turn on. By setting the flag to true CFME will try to set the "ems_created_on" column in the vms table after an ems refresh for new VMs and any VMs with a nil "ems_created_on" value. CFME looks at event information in our database as well as looking up historical event data from the management system. This is optional since the historical lookup could timeout. Default: false
collect_advanced_settings	Set to false if you do not want to collect advanced Virtual Machine settings during a management system refresh. This will increase the speed of the refresh, but less data will be collected. If the parameter is not listed, then the value is true. Default: true
ec2	
get_private_images	For EC2 refreshes only; whether or not to retrieve private images Default: true
get_public_images	For EC2 refreshes only; whether or not to retrieve public images Default: false Warning: setting get_public_images to **`true`** loads several thousand images in the VMDB by default and may cause performance issues.
get_shared_images	For EC2 refreshes only; whether or not to retrieve shared images. Default: true
ignore_terminated_instances	For EC2 refreshes only; whether or not to ignore terminated instances Default: true
full_refresh_threshold	The number of targeted refreshes requested before they are rolled into a full refresh. For example, if the system and/or the user target a refresh against 7 VMs and 2 Hosts (9 targets), when the refresh actually occurs it will do a partial refresh against those 9 targets only. However, if a 10th had been added, the system would perform a full EMS refresh instead Default: 100

Parameter	Description
raise_vm_snapshot_complete_if_created_within:	Raises vm_snapshot_complete event for a snapshot being added to VMDB only if the create time in Virtual Center is within the configured period of time. This prevents raising events for old snapshots when a new VC is added to CFME. Default: 15.minutes
refresh_interval	Scheduler does a periodic full EMS refresh every refresh_interval Default: 24.hours

Table 5.4. host_scan

Parameter	Description
queue_timeout	Time period after which a host SmartState analysis will be considered timed out.. Default: 20.minutes

Table 5.5. log

Parameter	Description
level	Specify the required level of logging for the CFME Appliance. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. This is the same as Log Level in Configuration-Operations- Server-Logging in the CFME Console and applies immediately to the evm.log file. Default: info
level_aws	Specify the level of logging for Amazon Web Services communications. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. This applies to the aws.log file. Default: info
level_aws_in_evm	Specify what level of Amazon Web Services communication log should be also shown in evm.log. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. Default: error

Parameter	Description
level_fog	Specify the level of logging for Fog communications. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. This applies to the fog.log file. Default: info
level_fog_in_evm	Specify what level of Fog communication log should be also shown in evm.log. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. Default: error
level_rails	Specify the level of logging for Rails. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. Once changed, this applies immediately to the production.log file. Default: info
level_rhevm	Specify the level of logging for Red Hat communications. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. This applies to the rhevm.log file. Default: warn
level_rhevm_in_evm	Specify what level of Red Hat communication log should be also shown in evm.log. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. Default: error
level_vim	Specify the level of logging for VIM (communication with VMware ESX and Virtual Center). Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. This applies to the vim.log file. Default: warn
level_vim_in_evm	Specify what level of vim logging should be also shown in evm.log. Possible levels from most detailed to least detailed are: debug, info, warn, error, fatal. Default: error

Table 5.6. db_stats

Parameter	Description

Parameter	Description
enabled	Specify if you want to keep track of the number of queries, size of queries, number of responses, size of response, min/max for each, number of established connections at for each server process. This information will show in the EVM log. Default: false
log_frequency	How frequently in seconds the process will log the database statistic in seconds. Default: 60

Table 5.7. callsites

Parameter	Description
enabled	Specify if you want keep track of the code that is accessing the database. Enabling call sites will decrease performance because of the amount of information tracked. The db_stats: enabled parameter must be set to true to use this. Default: false
depth	Specify how many levels in the call stack to track for each database access. Default: 10
min_threshold	Do not keep track of code that does not access the database this many times per log_frequency. Default: 10
path	Set the path for the CFME Appliance log. This is the same as Log Path in Configuration-Operations-Server-Logging in the CFME Console. Default: If no value is present, the path is /var/www/miq/vmdb/log.
line_limit	Limit how many characters are retained in a single log line. 0 means no limit. Default: 0

Table 5.8. collection

Parameter	Description
ping_depot	Whether to use TCP port ping to the log depot before performing log collection. Default: true

Parameter	Description
ping_depot_timeout	Specify how long in seconds to wait for response from log depot before deciding that the TCP port ping failed. Default: 20
current	When collecting logs, specifies what is considered current logging as opposed to archived logging. Default: :pattern: - log/*.log - log/apache/*.log - log/*.txt - config/* - /opt/rh/postgresql92/root/var/lib/pgsql/data/*.conf - /opt/rh/postgresql92/root/var/lib/pgsql/data/pg_log/* - /var/log/syslog* - /var/log/daemon.log* - /etc/default/ntp* - /var/log/messages* - /var/log/cron* - BUILD - GUID - VERSION
archive	Specifies what is considered archived logging. The default pattern is blank which means *.gz files in the log directory.

Table 5.9. log_depot

Parameter	Description
uri	Specify the uri for the log depot. This is the same as URI in Assistance-Collect Logs in the CFME Console. Default: blank

Parameter	Description
username	Specify the user name for the log depot. This is the same as User ID in Assistance-Collect Logs in the CFME Console. Default: blank
password	Specify the password for the user for the log depot. This is the same as Password in Assistance-Collect Logs in the CFME Console. Default: blank

Table 5.10. performance

Parameter	Description
capture_threshold	
vm	Amount of time in minutes to wait after capture before capturing again Default: 50.minutes
host	Amount of time in minutes to wait after capture before capturing again Default: 50.minutes
ems_cluster	Amount of time in minutes to wait after capture before capturing again Default: 50.minutes
storage	Amount of time in minutes to wait after capture before capturing again Default: 120.minutes
capture_threshold_with_alerts	
host	Amount of time in minutes to wait after capture before capturing again. This value is used instead of capture_threshold for Hosts that have alerts assigned based on real time Capacity & Utilization data. Default: 20.minutes
ems_cluster	Amount of time in minutes to wait after capture before capturing again. This value is used instead of capture_threshold for clusters that have alerts assigned based on real time Capacity & Utilization data. Default: 50.minutes

Parameter	Description
vm	Amount of time in minutes to wait after capture before capturing again. This value is used instead of capture_threshold for VMs that have alerts assigned based on real time Capacity & Utilization data. Default: 20.minutes
concurrent_requests	
hourly	Number of concurrent VC requests to make when capturing hourly raw metrics Default: 1
realtime	Number of concurrent VC requests to make when capturing real time raw metrics Default: 20
history	
initial_capture_days	How many days to collect data for on first collection Default: 0
Keep_daily_performances	How long to keep daily performance data in the VMDB Default: 6.months
keep_realtime_performances	How long to keep realtime performance data in the VMDB Default: 4.hours
keep_hourly_performances	How long to keep hourly performance data in the VMDB Default: 6.months
purge_window_size	When the purge needs to delete rows which are older than the keep_realtime_performances, keep_hourly_performances, and keep_daily_performances values, this value sets how many rows to delete in each batch. For example, a value of 1000 will cause us to issue ten 1,000 row deletes. Default: 1000

Table 5.11. repository_scanning

Parameter	Description
defaultsmartproxy	Specify the SmartProxy for repository scanning. This is the same as Default Repository Smartproxy in Configuration-Operations- Server-VM Server Control in the CFME Console. Default: blank

Table 5.12. server

Parameter	Description
case_sensitive_name_search	Specifiy if you want the search by name on configuration item screens to be case senstivite. Default: false
company	Specify the label you want to use for your company's tagging. This is the same as Company Name in Configuration-Operations- Server-Basic Info. Default: "My Company"
custom_logo	Specify if you want to use a custom logo. This is the same as Use Custom Logo in Configuration-Custom Logo-Logo Selection. Default: false
events	
disk_usage_gt_percent	For CFME operational alerts, specify at what threshold the disk usage alerts will be triggered. Default: 80
heartbeat_timeout	How long to wait until the server heartbeat is considered timed out. if the timeout is exceeded, other appliances in the zone/region can vie for the roles active on the timed out CFME Appliance. Default: 2.minutes
host	CFME Server's IP address Default: blank
hostname	CFME Server's hostname Default: localhost.localdomain
listening_port	Specify the port number on which the web server is listening. Note: This does not set the port that VMDB listens on. When deploying the SmartHost from the CFME Appliance, it tells the SmartHost (miqhost) what port to talk to the VMDB on. Default: "443"
mks_version	Specify the version of the VMware MKS Plugin to use for the VM Console. This is the same as VMware MKS Plugin Version in Configuration-Operations- Server-VM Console. Default : 2.1.0.0

Parameter	Description
name	Set the name to display for the CFME Appliance that you are logged on to in the CFME Console. This is the same as Appliance Name in Configuration-Operations- Server-Basic Information. Default : EVM
role	Specify the roles for this CFME Server, separated by commas without spaces. The possible values are automate, database_operations, database_synchronization, ems_inventory, ems_metrics_collector, ems_metrics_coordinator, ems_metrics_processor, ems_operations, event, notifier, reporting, scheduler, smartproxy, smartstate, user_interface, web_services. This is the same as Server Roles in Configuration-Operations- Server- Server Control. Default: database_operations, event, reporting, scheduler, smartstate, ems_operations, ems_inventory, user_interface, web_services
session_store	Where to store the session information for all web requests. The possible values are sql, memory, or cache. SQL stores the session information in the database regardless of the type of database server. Memory stores all the session information in memory of the server process. Cache stores the information in a memcache server. Default: cache
startup_timeout	The amount of time in seconds that the server will wait and prevent logins during server startup before assuming the server has timed out starting and will redirect the user to the log page after login. Default: 300
timezone	Set the timezone for the CFME Appliance. Default: UTC
vnc_port	If using VNC for remote console, the port used by VNC. Default: 5800

Parameter	Description
zone	Set the Zone for this appliance belongs. This is the same as Zone in Configuration-Operations- Server-Basic Information. Default : default
:worker_monitor	Starts and monitors the workers. Parameters specified here will override those set in the workers:default section.
poll	How often the worker monitor checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 15.seconds
miq_server_time_threshold	How much time to give the server to heartbeat before worker monitor starts to take action against non-responding server. Default: 2.minutes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 1
sync_interval	Time interval to sync active roles and configuration for all workers. Default: 30.minutes
wait_for_started_timeout	How long to wait for a started worker to heartbeat before considering the worker timed out. Default: 10.minutes
kill_algorithm	
name	Criteria used to start killing workers. Default: used_swap_percent_gt_value
value	Value of the criteria used. Default: 80
start_algorithm	
name	After server startup, criteria that must be met to decide if the CFME Server can start a new worker. Default: used_swap_percent_lt_value

Parameter	Description
value	Value of criteria used. Default: 60

Table 5.13. session

Parameter	Description
interval	Set the time interval in seconds for checking inactive sessions in CFME Console. Default: 60
timeout	Set the time period in seconds in which inactive console sessions are deleted. This is the same as Session Timeout in Configuration-Operations-Server-Authentication in the CFME Console. Default: 3600
memcache_server	If you choose memory for session_store, you need to specify the memcache_server to retrieve the session information from. Default: 127.0.1.1:11211
memcache_server_opts	Options to send to memcache server. : blank
show_login_info	Specify whether or not you want to see login info on start page. Default: true

Table 5.14. smartproxy_deploy

Parameter	Description
queue_timeout	Timeout for host smartproxy deploy job. Default: 30.minutes

Table 5.15. smtp

Parameter	Description
host	Specify the hostname of the smtp mail server. This is the same as Host in Configuration-Operations-Server-Outgoing SMTP E-mail Server. Default: localhost

Parameter	Description
port	Specify the port of the smtp mail server. This is the same as Port in Configuration-Operations-Server-Outgoing SMTP E-mail Server. Default: "25"
domain	Specify the domain of the smtp mail server. This is the same as Domain in Configuration-Operations-Server-Outgoing SMTP E-mail Server. Default: mydomain.com
authentication	Specify the type of authentication of the smtp mail server. This is the same as Authentication in Configuration-Operations-Server-Outgoing SMTP E-mail Server. Default: login
user_name	Specify the username required for login to the smtp mail server. This is the same as User Name in Configuration-Operations-Server-Outgoing SMTP E-mail Server. Default: evmadmin
password	Specify the encrypted password for the user_name account. This is the same as Password in Configuration-Operations-Server-Outgoing SMTP E-mail Server. Default: blank
from	Set the address that you want to send e-mails from. This is the same as From E-mail Address in Configuration-Operations-Server-Outgoing SMTP E-mail Server. Default: cfadmin@cfserver.com

Table 5.16. snapshots

Parameter	Description
create_free_percent	Ensures the % of free space available on the main datastore (datastore where vmx file is located) can support the % growth of the snapshot. The default is to require space for 100% of the provisioned size of all disks that are taking part in the snapshot. A value of 0 means do not check for space before creating the snapshot. Default: 100

Parameter	Description
remove_free_percent	Ensures the % of free space available on the main datastore (datastore where vmx file is located) has the % free space available to support the snapshot deletion process. Note that the deletion process consists of first composing a new snapshot then removing it once the original snapshot to be deleted has been collapsed in the VM. The default is to require 100% of the size of all disks to complete this process. A value of 0 means do not check for space before removing the snapshot. Default: 100

Table 5.17. webservices

Parameter	Description
contactwith	Set to ipaddress to contact miqhost using the IP address. Set to hostname to contact miqhost by its hostname. Set to resolved_ipaddress to take the hostname and resolve it to an IP address. Default: ipaddress
mode	Set to invoke to use webservices. Set to disable to turn off webservices. This is the same as Mode in Configuration-Operations- Server-Web Services in the CFME Console. Default: invoke
nameresolution	If set to true, the hostname will be resolved to an IP address and saved with the host information in the VMDB. Default: false
security	If Web Services are enabled, you can set this to ws-security. This is the same as Security in Configuration-Operations- Server-Web Services in the CFME Console. Note: This is not currently supported. Default: none
timeout	Specify the web service timeout in seconds. Default: 120

Parameter	Description
use_vim_broker	Controls if the vim_broker is used to communicate with VMware infrastructure. Default: true

Table 5.18. workers

Parameter	Description
worker_base	
defaults	If the following parameters are NOT explicitly defined for a specific worker, then these values will be used.
count	Number of this type of worker. Default: 1
gc_interval	How often to do garbage collection for this worker. Default: 15.minutes
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 3.seconds
poll_method	If set to normal, the worker checks for work the number of seconds set in the poll parameter. If set to escalate, the worker will increase the time between checks when there is no work to be done. Default: normal
poll_escalate_max	The maximum number of time to wait between checks for work. Poll_method must be set to escalate for this option to be used. Default: 30.seconds
heartbeat_freq	How often to "heartbeat" the worker Default: 60.seconds
heartbeat_method	Set which way to dispatch work. Possible values are sql or drb. Default: drb

Parameter	Description
heartbeat_timeout	How long to wait until the worker heartbeat is considered timed out Default: 2.minutes
parent_time_threshold	How long to allow the parent to go without heartbeating before considering the "parent' not responding. For workers, the worker monitor is the parent. For Worker monitor, the Server is the parent. Default: 3.minutes
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 150.megabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 10
restart_interval	How long to let a worker remain up before asking it to restart. All queue based workers are set to 2.hours and every other worker does not get restarted by a 0.hours value. Default: 0.hours
starting_timeout	How long to wait before checking a worker's heartbeat when it is starting up to mark it as not reponding, similar to a grace period before you begin monitoring it. Default: 10.minutes
event_catcher	Associated with Event Monitor Server Role. Captures ems events and queues them up for the event_handler to process. Parameters specified here will override those set in the worker_base:default section.
ems_event_page_size	Internal system setting which sets the maximum page size for the event collector history. This should not be modified. Default: 100
ems_event_thread_shutdown_timeout	Internal system setting which determines how long the event catcher at shutdown will wait for the event monitor thread to stop. This should not be modified. Default: 10.seconds

Parameter	Description
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 2.gigabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 1
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 1.seconds
event_catcher_redhat	Contains settings that supersede the event_catcher for event_catcher_redhat.
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 15.seconds
event_catcher_vmware	Contains settings that supersede the event_catcher for event_catcher_vmware.
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 1.seconds
event_catcher_openstack	Contains settings that supersede the event_catcher for event_catcher_openstack.

Parameter	Description
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 15.seconds
topics	List of AMQP topics that should be monitored by CFME when gathering events from Openstack.
duration	Qpid Specific. Length of time (in seconds) the receiver should wait for a message from the Qpid broker before timing out. Default: 10.seconds
capacity	Qpid Specific. The total number of messages that can be held locally by the Qpid client before it needs to fetch more messages from the broker. Default: 50.seconds
amqp_port	Port used for AMQP. Default: 5672
replication_worker:	Performs database replication tasks. Settings for Database Synchronization Server Role. Parameters specified here will override those set in the queue_worker_base:default section.
connection_pool_size	Maximum number of database connections allowed per process. Default: 5
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 200.megabytes
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 60.seconds
replication:	This section contains information for the destination database for the replication.

Parameter	Description
destination:	
database	Name of destination database. Default: vmdb_production
username: root	Username for the destination database. Default: root
password	Stores password for destination database in encrypted format.
host	Host of the destination database.
port	Port of the destination database. Default: 5432
include_tables	Lists tables included in the replication. Do NOT modify unless specifically instructed to do so by ManageIQ support. Default: include all, exclude_tables is used instead.
exclude_tables	Lists tables not to be included in the replication. Do NOT modify unless specifically instructed to do so by ManageIQ support.
options	
replication_trace	Set to true to capture all replication tracing in the log. Default: false
schedule_worker	Settings for Scheduler Server Role and any other work that runs on a schedule. Parameters specified here will override those set in the worker_base:default section.
db_diagnostics_interval	How frequently to collect database diagnostics statistics Default: 30.minutes
job_proxy_dispatcher_interval	How often to check for available SmartProxies for SmartState Analysis jobs. Default: 15.seconds
job_proxy_dispatcher_stale_message_check_interval	How often to check for the dispatch message in the queue Default: 60.seconds
job_proxy_dispatcher_stale_message_timeout	Kill a message if this value is reached. Default: 2.minutes
job_timeout_interval	How often to check to see if a job has timed out. Default: 60.seconds

Parameter	Description
license_check_interval	How often to check for valid license. Default: 1.days
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 150.megabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 3
performance_collection_interval	Controls how often the schedule worker will put performance collection request on the queue to be picked up by the collection worker. Default: 3.minutes
performance_collection_start_delay	How long after CFME Server has started before starting capacity and utilization collection, if collection needs to be done. Default: 5.minutes
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 15.seconds
server_logs_stats_interval	How often to log the CFME Server statistics. Default: 5.minutes
server_stats_interval	How often to collect the CFME Server statistics. Default: 60.seconds
session_timeout_interval	How often to check to see if a UI (CFME Console) session has timed out. Default: 30.seconds
storage_file_collection_interval	How often to perform file inventory of storage locations. Default: 1.days

Parameter	Description
storage_file_collection_time_utc	What time to perform file inventory of storage locations. Default: "06:00"
vdi_refresh_interval	How often to refresh vdi inventory Default: 20.minutes
vm_retired_interval	How often to check for virtual machines that should be retired. Default: 10.minutes
vm_scan_interval	How often to check virtual machines to see if scan needs to be done. Default: 10.minutes
smis_refresh_worker	Settings for Storage Inventory Server Role and any other work that runs on a schedule. Parameters specified here will override those set in the worker_base:default section
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 15.seconds
connection_pool_size	Maximum number of database connections allowed per process. Default: 5
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 1.gigabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 3
smis_update_period	How frequently to update smis information. Default: 1.hours
status_update_period	How frequently to update smis status. Default: 5.minutes

Parameter	Description
stats_update_period	How frequently to update smis statistics. Default: 10.minutes
vim_broker_worker	Launched for any of these roles: Capacity & Utilization Collector, SmartProxy, SmartState Analysis, Management System Operations, Management System Inventory. Also launched if the use_vim_broker setting is on. Provides connection pooling, caching of data to and from the VMware infrastructure. Parameters specified here will override those set in the workers:default section.
heartbeat_freq	How often to heartbeat the worker Default: 15.seconds
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 1.gigabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 3
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 1.seconds
reconnect_retry_interval	Period after which connection is retried. Default: 5.minutes
vim_broker_status_interval	Interval at which the status of the vim_broker is checked. Default: 15.minutes
vim_broker_update_interval	Internal system setting which configures how much time to wait after receiving event updates before checking for more updates. Default: 0.seconds
wait_for_started_timeout	Time between the worker's preload and startup time before considering the worker timed out. Default: 10.minutes

Parameter	Description
ui_worker:	Settings for User Interface Server Role. Parameters specified here will override those set in the worker_base:default section.
connection_pool_size	Maximum number of database connections allowed per process. Default: 5
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 1.gigabytes
nice_delta: 1	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 1
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 60.seconds
web_service_worker:	Settings for Web Services Server Role. Parameters specified here will override those set in the worker_base:default section.
connection_pool_size	Maximum number of database connections allowed per process. Default: 5
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 1.gigabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 1

Parameter	Description
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 60.seconds
queue_worker_base	Base class of all queue workers that work off of the queue..
defaults	If the following parameters are NOT explicitly defined for a queue worker, then these values will be used.
cpu_usage_threshold	How much cpu to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 100.percent
queue_timeout	How long a queue message can be worked on before it is considered timed out. Default: 10.minutes
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 400.megabytes
restart_interval	Queue workers restart interva.l Default: 2.hours
poll_method	If set to normal, the worker checks for work the number of seconds set in the poll parameter. If set to escalate, the worker will increase the time between checks when there is no work to be done. Default: normal
generic_worker	Performs work that is not classified as any specific type of work. Processes all normal priority or non-specific queue items. Parameters specified here will override those set in the queue_worker_base:default section
count	Number of this type of worker. Default: 4
ems_refresh_worker	Performs all ems (management system) refreshes to keep the vmdb in sync with the state of the components of the virtual infrastrucutre in the various management systems. Parameters specified here will override those set in the queue_worker_base:default section

Parameter	Description
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 10.seconds
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 2.gigabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 7
restart_interval	Queue workers restart interval. Default: 2.hours
queue_timeout	How long a message can be worked on before it is considered timed out. Default: 120.minutes
event_handler	Associated with Event Monitor Server Role. Handles all events caught by the event catcher worker. Parameters specified here will override those set in the workers:default section. Parameters specified here will override those set in the queue_worker_base:default section
cpu_usage_threshold	How much cpu to allow the worker to grow to before gracefully requesting it to exit and restart. The value of 0 means that this worker will never be killed due to CPU usage. Default: 0.percent
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 7
perf_collector_worker	Connects to VC/ESX to collect the raw performance data. Same as the Capacity & Utilization Data Collector Server Role. Parameters specified here will override those set in the queue_worker_base:default section

Parameter	Description
count	Number of this type of worker. Default: 2
poll_method	If set to normal, the worker checks for work the number of seconds set in the poll parameter. If set to escalate, the worker will increase the time between checks when there is no work to be done. Default: escalate
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 3
perf_processor_worker	Processes the raw performance data into a reportable format. Same as the Capacity & Utilization Data Processor Server Role. Parameters specified here will override those set in the queue_worker_base:default section
count	Number of this type of worker. Default: 2
poll_method	If set to normal, the worker checks for work the number of seconds set in the poll parameter. If set to escalate, the worker will increase the time between checks when there is no work to be done. Default: escalate
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 400.megabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 7
priority_worker	Performs all high priority queue items including many tasks on behalf of the UI. UI requests are normally executed by a priority worker so they will not to block the UI. Parameters specified here will override those set in the queue_worker_base:default section
count	Number of this type of worker. Default: 2

Parameter	Description
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 200.megabytes
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 1
poll	How often the workers checks for work. This value only is only used when the worker has no more work to do from the queue. It will wait for an amount of time determined by the poll value and poll method. Therefore, if there is constant work on the queue, the worker will not wait in between messages. Default: 1.seconds
reporting_worker	Compiles reports. Settings for Reporting Server Role. Parameters specified here will override those set in the queue_worker_base:default section
count	Number of this type of worker. Default: 2
nice_delta	Tells the worker monitor what Unix "nice" value to assign the workers when starting. A lower number is less nice to other processes. Default: 7
smart_proxy_worker	Performs the embedded scanning of virtual machines. Settings for SmartProxy Server Role. Parameters specified here will override those set in the queue_worker_base:default section
count	Number of this type of worker. Default: 3
memory_threshold	How much memory to allow the worker to grow to before gracefully requesting it to exit and restart. Default: 600.megabytes
queue_timeout	How long a queue message can be worked on before it is considered timed out. Default: 20.minutes
restart_interval	Queue workers restart interval. Default: 2.hours

5.1.5. Schedules

5.1.5.1. Scheduling SmartState Analyses and Backups

From the **Schedules** area in **Settings** you can schedule the analyses of virtual machines, hosts, clusters, and datastores to keep the information current. Depending on which resource you want to analyze, you can filter which ones to analyze. You may also specify only one virtual machine or perform an analysis on all virtual machines. In addition, you can schedule compliance checks, and database backups.

5.1.5.2. Scheduling a SmartState Analysis or Compliance Check

Procedure 5.32. To Schedule a SmartState Analysis or Compliance Check

1. Navigate to **Configure** → **Configuration**.

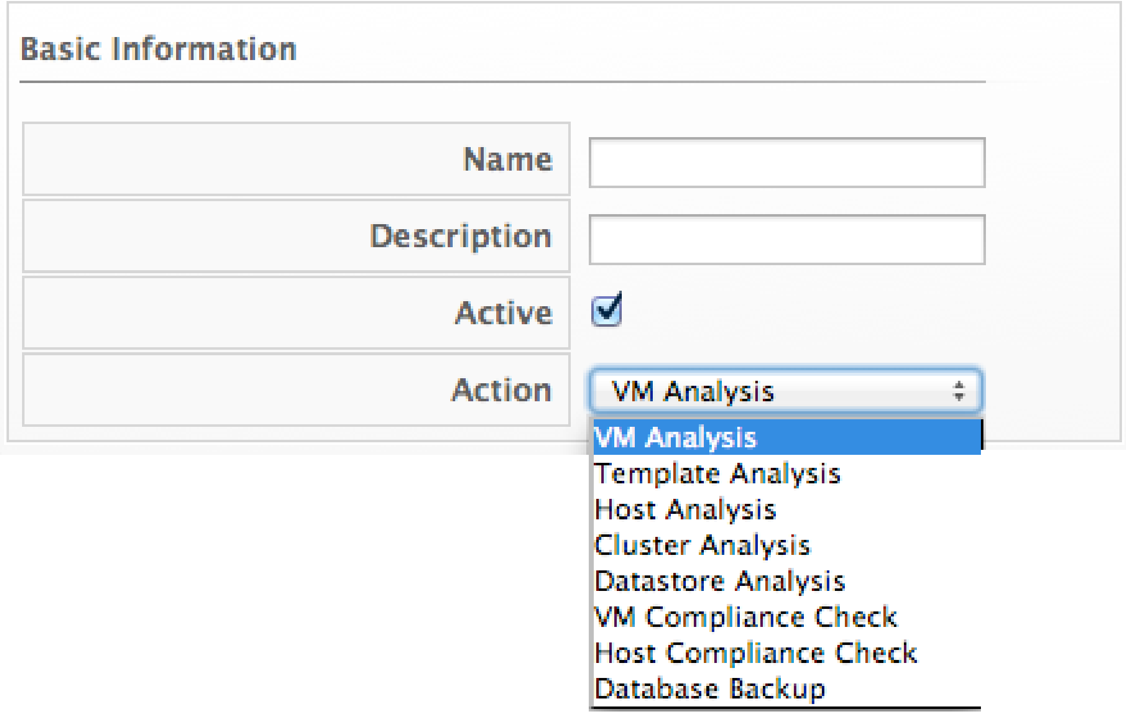
2. Click on the **Settings** accordion, then click **Schedules**.

3. Click ⚙ (**Configuration**), and + (**Add a new Schedule**).

4. In the **Basic Information** area, type in a **Name** and **Description** for the schedule.

5. Check **Active** if you want to enable this scan.

6. From the **Action** dropdown, select the type of analysis you want to schedule. Based on the type of analysis you choose, you are presented with one of the following group boxes.



Basic Information

Name	
Description	
Active	☑
Action	VM Analysis

- **VM Analysis**: Displays **VM Selection** where you can choose to analyze **All VMs**, **All VMs for Provider**, **All VMs for Cluster**, **All VMs for Host**, **A single VM**, or **Global Filters**.

- **Template Analysis**: Displays **Template Selection** where you can choose to analyze **All Templates**, **All Templates for Provider**, **All Templates for Cluster**, **All Templates for Host**, **A single Template**, or **Global Filters**.

- **Host Analysis**: Displays **Host Selection** where you can choose to analyze **All Hosts**, **All Hosts for Provider**, **A single Host**, or **Global Filters**.

> **Note**
>
> You can only schedule host analyses for connected virtual machines, not repository virtual machines that were discovered through that host. Since repository virtual machines do not retain a relationship with the host that discovered them, there is no current way to scan them through the scheduling feature. The host is shown because it may have connected virtual machines in the future when the schedule is set to run.

- **Cluster Analysis**: Displays **Cluster Selection** where you can choose to analyze **All Clusters**, **All Clusters for Provider**, or **A single Cluster**.

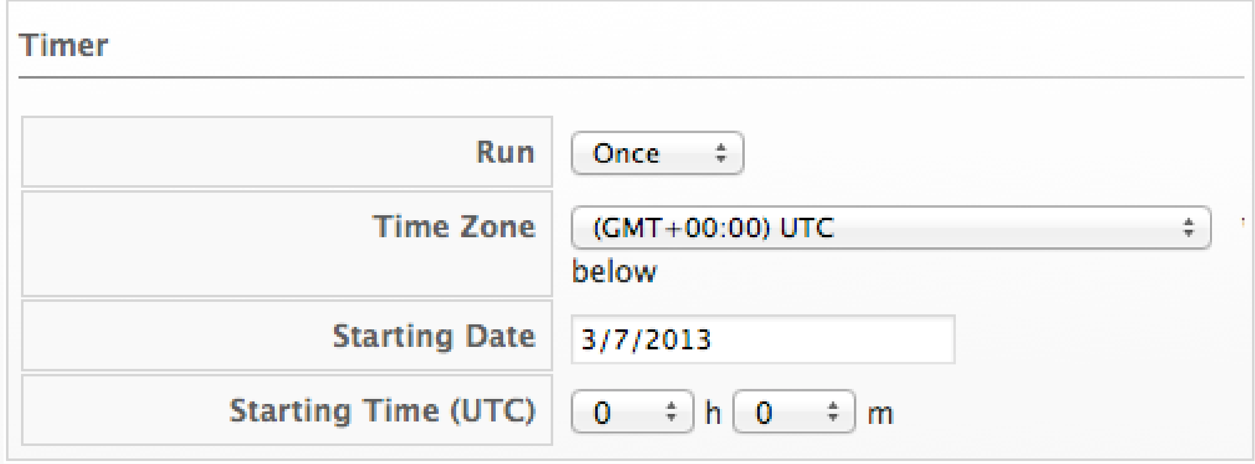
- **Datastore Analysis**: Displays **Datastore Selection** where you can choose to analyze **All Datastores**, **All Datastores for Host**, **All Datastores for Provider**, **A single Datastore**, or **Global Filters**.

- **VM Compliance Check**: Displays **VM Selection** where you can choose to analyze **All VMs**, **All VMs for Provider**, **All VMs for Cluster**, **All VMs for Host**, **A single VM**, or **Global Filters**.

- **Host Compliance Check**: Displays **Host Selection** where you can choose to analyze **All Hosts**, **All Hosts for Provider**, **All Hosts for Cluster**, **A single Host**, or **Global Filters**.

7. By applying **Global Filters** within any of the above items, you can designate which virtual machines or hosts to analyze.

8. In the **Timer** area, click the **Run** dropdown to set the frequency of the analysis to run. There are further options based on which **Run** option you choose.



Timer

Run	Once
Time Zone	(GMT+00:00) UTC below
Starting Date	3/7/2013
Starting Time (UTC)	0 h 0 m

- Click **Once** to have the analysis run just one time.

- Click **Daily** to run the analysis on a daily basis. You will be prompted to select how many days you want between each analysis.

- Click **Hourly** to run the analysis hourly. You will be prompted to select how many hours you want between each analysis.

9. Select a **Time Zone**. Note that if you change the **Time Zone**, you will need to reset the stating date and time.

10. Type or select a date to begin the schedule in **Starting Date**.

11. Select a **Starting Time** based on a 24 hour clock in the selected **Time Zone**.

12. Click **Add**.

5.1.5.3. Scheduling a Database Backup

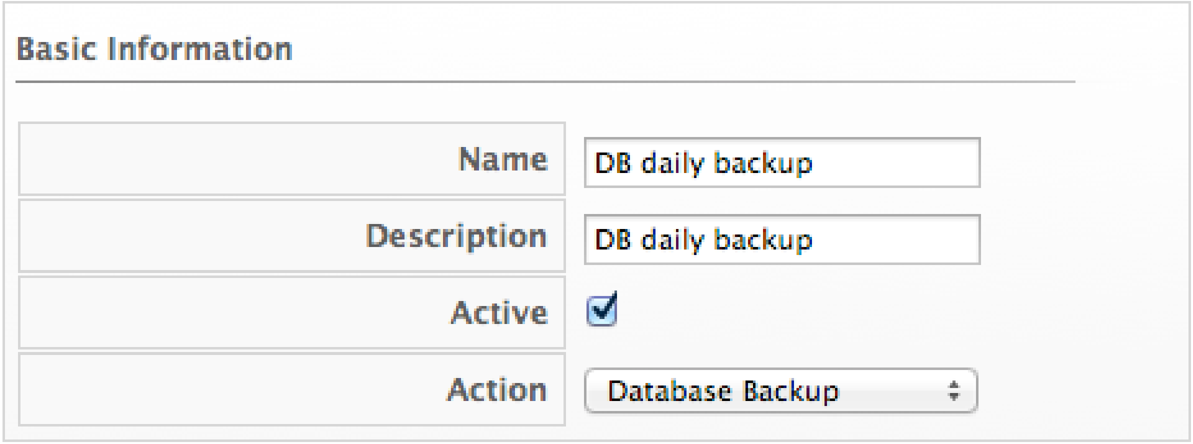
Procedure 5.33. To Schedule a Database Backup

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Settings** accordion, then click **Schedules**.

3. Click ⚙ (**Configuration**), and ✚ (**Add a new Schedule**).

4. In the **Basic Information** area, type in a **Name** and **Description** for the schedule.



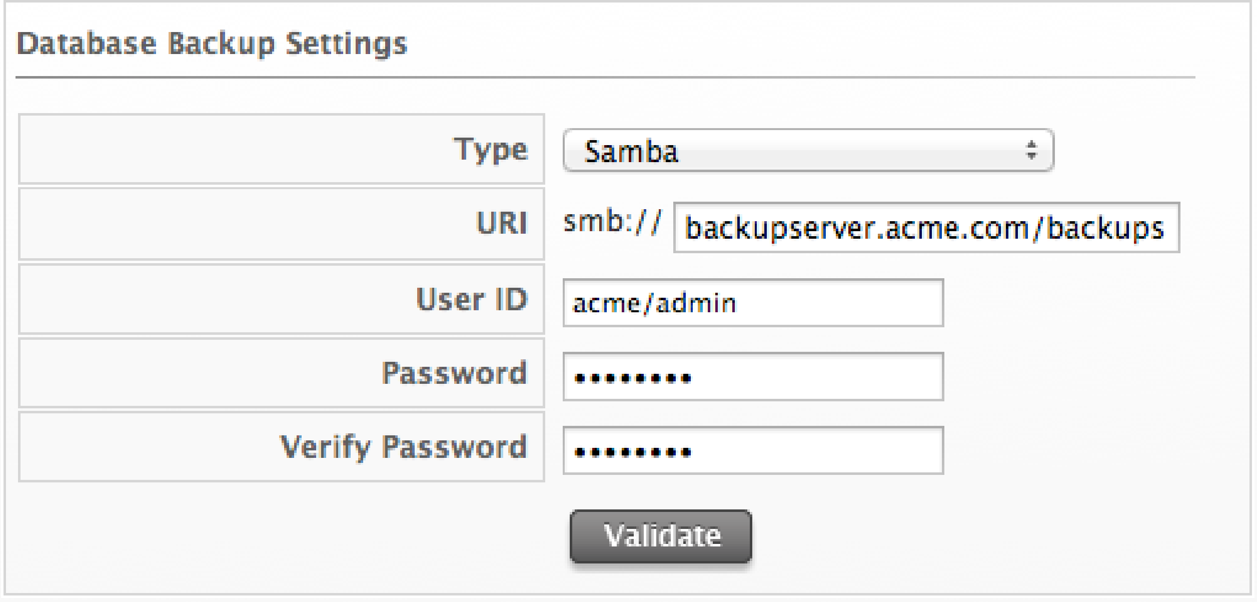
Basic Information

Name	DB daily backup
Description	DB daily backup
Active	☑
Action	Database Backup

5. Check **Active** if you want to enable this backup schedule.

6. From the **Action** dropdown, select **Database backup**.

7. In the **Database Backup Settings** area, select a type of server to put the backups. You can either use **Network File System** or **Samba**.

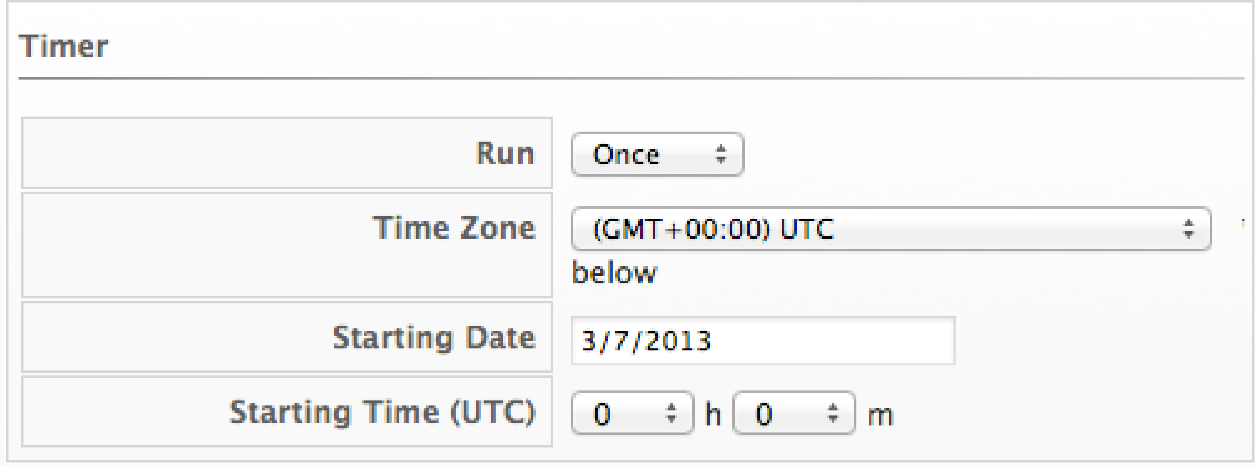


Database Backup Settings

Type	Samba
URI	smb:// backupserver.acme.com/backups
User ID	acme/admin
Password	••••••••
Verify Password	••••••••

- If selecting **Samba**, enter the **URI**, **User ID**, and a valid **Password**. Then, click **Validate** to check the settings.
- If you choose **Network File System**, enter the **URI**.

8. In the **Timer** area, click the **Run** dropdown to specify how often you want the analysis to run. Your options after that will depend on which **Run** option you choose.



Timer

Run	Once
Time Zone	(GMT+00:00) UTC below
Starting Date	3/7/2013
Starting Time (UTC)	0 h 0 m

- Click **Once** to have the backup run just one time.
- Click **Daily** to run the backup on a daily basis. You will be prompted to select how many days you want between each analysis.
- Click **Hourly** to run the backup hourly. You will be prompted to select how many hours you want between each analysis.

9. Select a **Time Zone**. Note that if you change the **Time Zone**, you will need to reset the stating date and time.
10. Type or select a date to begin the schedule in **Starting Date**.
11. Select a **Starting Time (UTC)** based on a 24 hour clock in the selected time zone.
12. Click **Add**.

5.1.5.4. Modifying a Schedule

5.1.5.4. Modifying a Schedule

Procedure 5.34. To Modify a Schedule

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Settings** accordion, then click **Schedules**.
3. Click the schedule that you want to edit.
4. Click ⚙ (**Configuration**), and then click ✎ (**Edit this Schedule**).
5. Make the required changes.
6. Click **Save**.

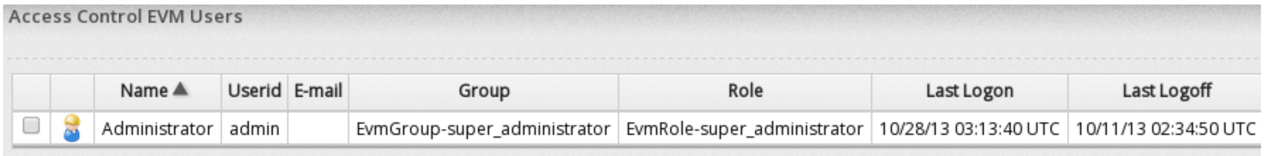
5.2. Access Control

From navigating to **Configure** → **Configuration**, then clicking on the **Access Control** accordion, you have a hierarchy of the configurable items for users, groups, and roles. You can add and modify users, groups, and account roles.

5.2.1. Creating a User

Procedure 5.35. To Create a User

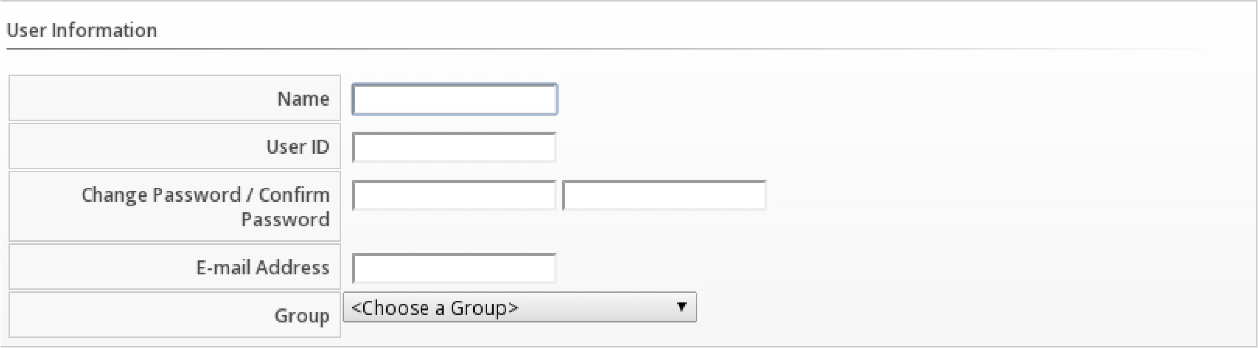
1. Navigate to **Configure** → **Configuration**.
2. Click on the **Access Control** accordion, then click **Users**.



Access Control EVM Users

		Name ▲	Userid	E-mail	Group	Role	Last Logon	Last Logoff
☐		Administrator	admin		EvmGroup-super_administrator	EvmRole-super_administrator	10/28/13 03:13:40 UTC	10/11/13 02:34:50 UTC

3. Click ⚙ (**Configuration**), and ➕ (**Add a new User**) to create a user.
4. Type in a **Name**, **UserID**, **Password** with confirmation, and **Email Address** for the user.



User Information

Name	
User ID	
Change Password / Confirm Password	
E-mail Address	
Group	<Choose a Group> ▾

> **Note**
>
> If you are using LDAP, but did not enable **`Get User Groups from LDAP`** in your server's **`Authentication`** tab, you will need to define a user. The UserID must match exactly the user's name as defined in your directory service. Use all lowercase to be sure that the user can be found in the VMDB. For example, *jdunn@acme.com* when using User Principal Name, *cn=Jack Dunn,ou=users,dc=acme,dc=com* when using Distinguished Name (*CN=<user>*), or *uid=Jack Dunn,ou=users,dc=acme,dc=com* when using Distinguished Name (*UID=<user>*). Then, when logging in, the user would type either *jdunn* for User Principal Name or *Jack Dunn* for Distinguished Name. If the user is not defined in the VMDB, they will be denied access to CloudForms Management Engine. The password field will not be used. When the user logs in they should use their LDAP password.

5. Select a **`Group`**.

6. Click **`Add`**.

5.2.2. Deleting a User

For security reasons, delete any user that no longer needs access to the information or functions of the server

Procedure 5.36. To Delete a User

1. Navigate to **Configure** → **Configuration**.

2. Click on the **`Access Control`** accordion, then click **`Users`**.

3. Select the user you want to delete.

4. Click ⚙ (**`Configuration`**), and 🗑 (**`Delete selected Users`**) to delete a user.

5.2.3. Groups

User groups create filters and assign roles to users. You can either create your own user groups or leverage your LDAP directory service to assign groups of users to account roles. For a list of what each pre-defined account role can do, see *Roles*.

5.2.4. Creating a User Group

Procedure 5.37. To Create a User Group

1. Navigate to **Configure** → **Configuration**.

2. Click on the **`Access Control`** accordion, then click **`Groups`**.

3. Click ⚙ (**`Configuration`**), and ✚ (**`Add a new Group`**) to create a group.

4. Enter a name for the group in the **`Description`** field. To ensure compatibility with tags, use underscores in place of spaces. For example, **`CloudForms-test_group`**.

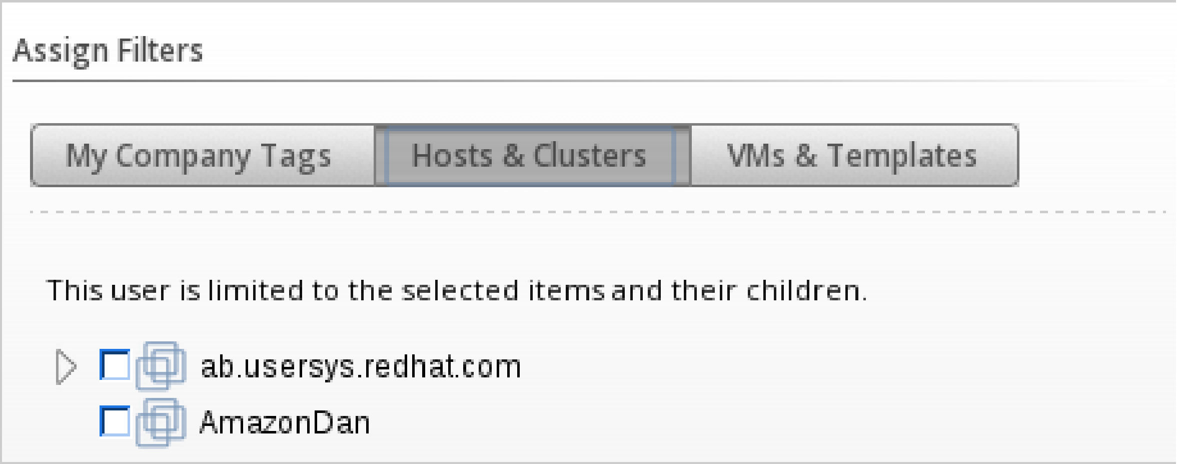
5. Select a role to map to this group.

6. Select any filters that you want applied to what this group can view in the **Assign Filters** area.

7. Check the boxes for the filters you want applied to this user. The items that have changed will show in a bold, blue font.

8. Click the **Host & Clusters** tab.

9. Check the boxes for the host and clusters that you want to limit this user to. The items that have changed will show in a bold, blue font.



Assign Filters

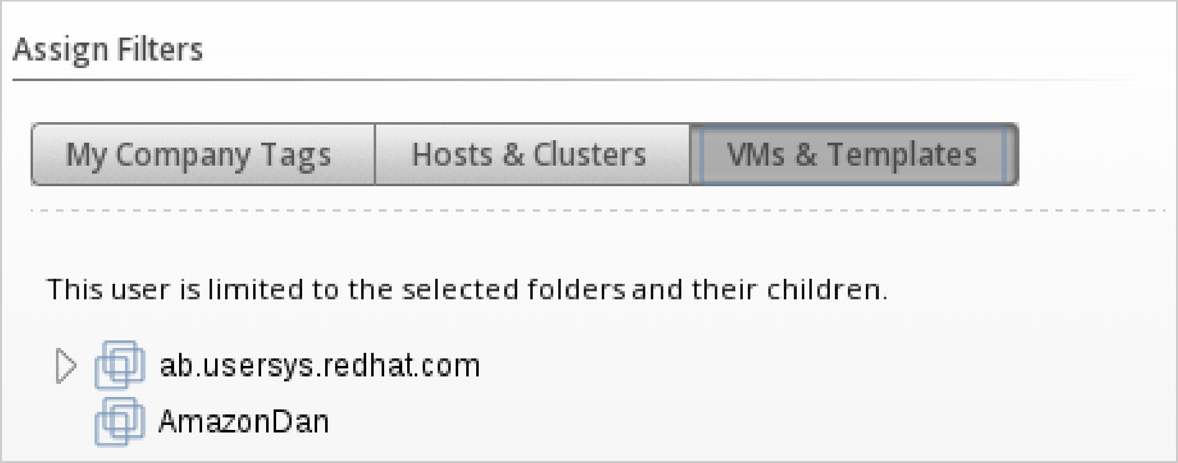
This user is limited to the selected items and their children.

□ ab.usersys.redhat.com

□ AmazonDan

10. Click the **VMs & Templates** tab. This shows folders that you have created in your virtual infrastructure.

11. Check the boxes for the folders that you want to limit this user to. The items that have changed will show in a bold, blue font.



Assign Filters

This user is limited to the selected folders and their children.

ab.usersys.redhat.com

AmazonDan

12. Click **Add**.

5.2.5. LDAP Groups

When leveraging your LDAP groups, if you are using LDAP and the LDAP user is not a member of any of the defined groups, then the user will be denied access to CloudForms Management Engine. There are two ways to use LDAP groups with CloudForms Management Engine:

- Create groups with a specific set of names as provided by CloudForms Management Engine. These groups automatically get assigned to a specific role.

- Assign pre-existing groups from your LDAP server to CloudForms Management Engine account roles.

5.2.6. Using CloudForms Management Engine's Named Groups to Assign Account Roles

In your directory service, define a distribution group for each of the account roles with the names shown in the table below. This group must be in the LDAP directory source you specified for the Server. See LDAP Settings.

5.2.7. Account Role and Directory Service Group Names

Directory Service Distribution Group Name	Account Role
EvmGroup-administrator	Administrator
EvmGroup-approver	Approver
EvmGroup-auditor	Auditor
EvmGroup-desktop	Desktop
EvmGroup-operator	Operator
EvmGroup-security	Security
EvmGroup-super_administrator	Super Administrator
EvmGroup-support	Support
EvmGroup-user	User
EvmGroup-user_limited_self_server	User Limited Self Service
EvmGroup-user_self_service	User Self Service
EvmGroup-vm_user	Vm User

1. Make each user of your directory service that you want to have access to CloudForms Management Engine a member of one of these groups.

2. Navigate to **Configure** → **Configuration**, then click on the **Settings** accordion, then **Zones**, then the **Authentication** tab, you can enable **Get User Groups from LDAP** after typing in all of the required settings. See *LDAP Settings*.

5.2.8. Using Pre-existing LDAP Groups to Assign Account Roles

Procedure 5.38. To Use Pre-existing LDAP Groups to Assign Account Roles

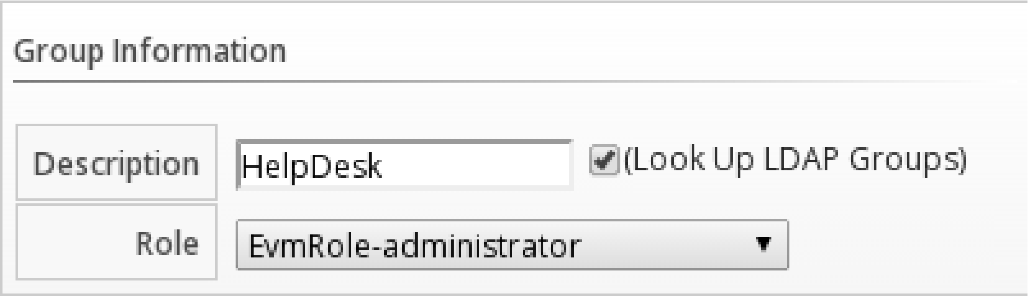
1. Navigate to **Configure** → **Configuration**.

2. Click on the **Access Control** accordion, then click **Groups**.

3. Click ⚙ (**Configuration**), and + (**Add a new Group**) to create a group.

4. There are two ways to specify which group you want to use:

   - Type in the cn for the group in LDAP Group. This group must be in the LDAP directory source you specified under Operations-Server.

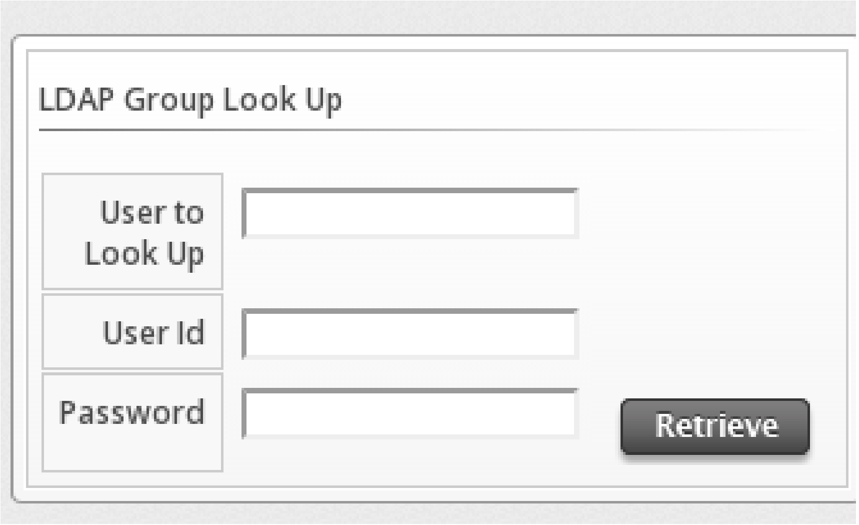


Group Information

Description: HelpDesk ☑ (Look Up LDAP Groups)

Role: EvmRole-administrator

- Or check **Look Up LDAP Groups** to find a list of groups, and then use the dropdown that appears in the LDAP **Group Information** area to choose a group.



LDAP Group Look Up

User to Look Up:

User Id:

Password:

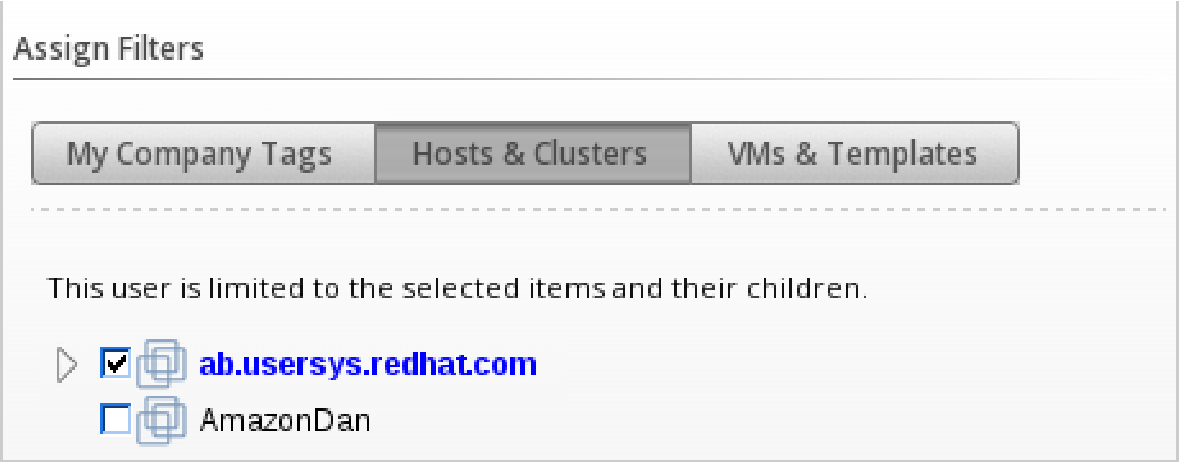
5. Select a **Role** to map to this group.

6. Select any filters that you want applied to what this group can view in the **Assign Filters** area.

7. Check the boxes for the filters you want applied to this user. The items that have changed will show in a bold, blue font.

8. Click the **Host & Clusters** tab.

9. Check the boxes for the host and clusters that you want to limit this user to. The items that have changed will show in a bold, blue font.



Assign Filters

This user is limited to the selected items and their children.

☑ **ab.usersys.redhat.com**

□ AmazonDan

10. Click the **VMs & Templates** tab. This shows folders that you have created in your virtual infrastructure.

11. Check the boxes for the folders that you want to limit this user to. The items that have changed will show in a bold, blue font.

12. Click **Add**.

5.2.9. Roles

When you create a user group, you must specify a role to give the group rights to resources in the console, and then assign a user to a group. CloudForms Management Engine provides a default group of roles, but you can also create your own as well as copy the default groups. The table below shows the function available to each group.

Note

If you have enabled **Get Role from LDAP** under LDAP Settings, then the role is determined by the LDAP users group membership in the directory service. See LDAP Settings

5.2.10. Account Roles and Descriptions

Role	Description
Administrator	Administrator of the virtual infrastructure. Can access all infrastructure functionality. Cannot change server configuration.
Approver	Approver of processes, but not operations. Can view items in the virtual infrastructure, view all aspects of policies and assign policies to policy profiles. Cannot perform actions on infrastructure items.
Auditor	Able to see virtual infrastructure for auditing purposes. Can view all infrastructure items. Cannot perform actions on them.
Desktop	Access to VDI pages.
Operator	Performs operations of virtual infrastructure. Can view and perform all functions on virtual infrastructure items including starting and stopping virtual machines. Cannot assign policy, but can view policy simulation from Virtual Machine page.
Security	Enforces security for the virtual environment. Can assign policies to policy profiles, control user accounts, and view all parts of virtual infrastructure. Cannot create policies or perform actions on virtual infrastructure.
Super Administrator	Administrator of CloudForms Management Engine and the virtual infrastructure. Can access all functionality and configuration areas.

Role	Description
Support	Access to features required by a support department such as diagnostics (logs). Can view all infrastructure items and logs. Cannot perform actions on them.
User	User of the virtual infrastructure. Can view all virtual infrastructure items. Cannot perform actions on them.
User Limited Self Service	Limited User of virtual machines. Can make provision requests. Can access some functions on the virtual machine that the user owns including changing power state.
User Self Service	User of virtual machines. Can make provision requests. Can access some functions on the virtual machine that the user owns and that the user's LDAP groups own including changing power state.
VM User	User of virtual machines. Can access all functions on the virtual machine including changing power state and viewing its console. Cannot assign policy, but can view policy simulation from virtual machine page.

5.2.11. Creating a Role

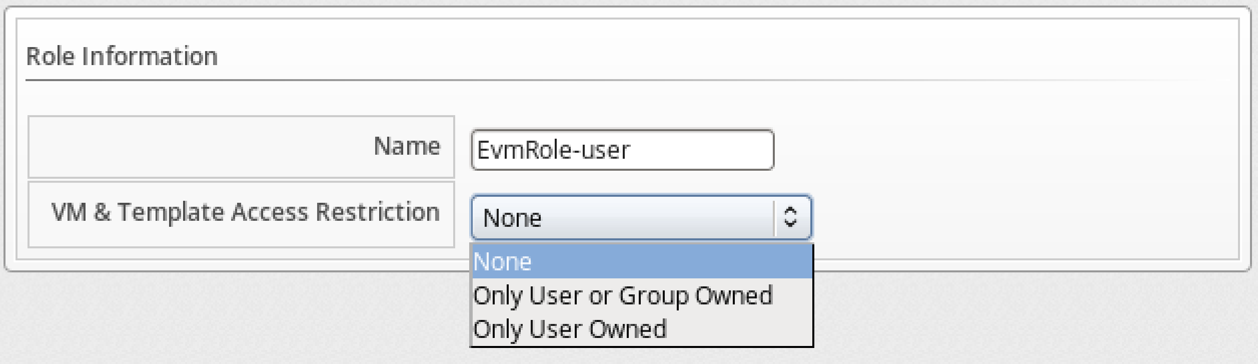
Procedure 5.39. To Create a Role

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Access Control** accordion, then click **Roles**.

3. Click ⚙ (**Configuration**), and ➕ (**Add a new Role**).

4. In the **Role Information** area, type a name for the new role. For **VM & Template Access Restriction**, select if you want to limit users with this role to only see virtual machines specifically used by the user, by the user or its group, or all virtual machines.

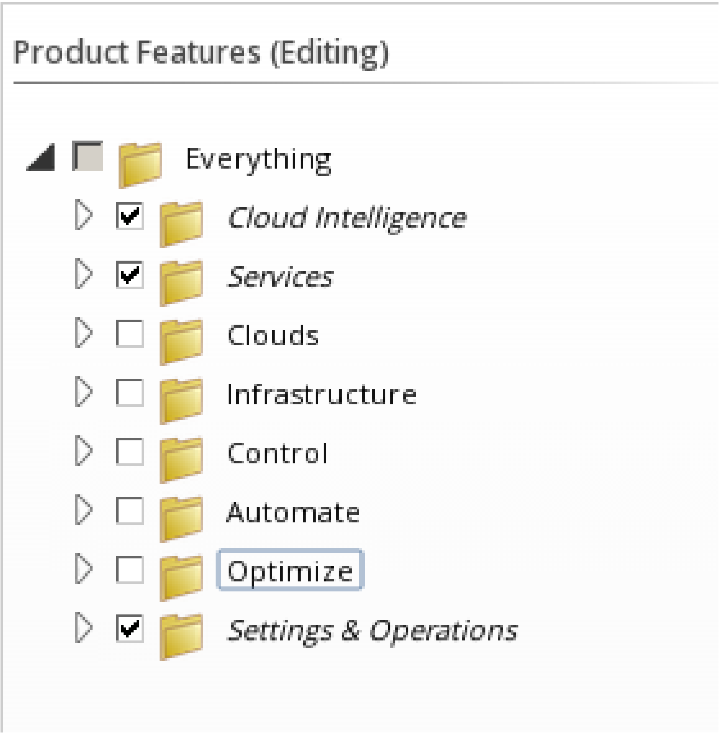


Role Information

Name: EvmRole-user

VM & Template Access Restriction: None

5. Under **Product Features (Editing)**, navigate to the appropriate feature and enable or disable it.



Product Features (Editing)

- ◢ ▣ Everything
  - ▷ ☑ *Cloud Intelligence*
  - ▷ ☑ *Services*
  - ▷ □ Clouds
  - ▷ □ Infrastructure
  - ▷ □ Control
  - ▷ □ Automate
  - ▷ □ Optimize
  - ▷ ☑ *Settings & Operations*

6. Click **Add**.

5.3. Diagnostics

From navigating to **Configure** → **Configuration**, then clicking on the **Diagnostics** tab, you can also see the status of the different CloudForms Management Engine roles and workers for each server, view and collect logs, and gather data if there are any gaps in capacity and utilization information. The **Diagnostics** area is designed in a hierarchy.

- At the *region* level, you can see replication status, backup the VMDB, and run garbage collection on the VMDB.
- At the *zone* level, you can see CloudForms Management Engine roles by servers and servers by roles. In addition, you can set log collection values for a specific zone, and collect gap data for capacity and utilization.
- At the *server* level, you can see the workers for each server, set log collection values for a specific server, and view current logs.

5.3.1. Region Diagnostics

Using the console, set the priority of server regional roles, can check and reset replication, and create backups of your database either on demand or on a schedule.

Regions are used primarily to consolidate multiple VMDBs into one master VMDB for reporting while zones are used to define functional groups of servers. There can be only one region per VMDB, but multiple zones per region (or VMDB). Some server roles are aware of each other across CloudForms Management Engine Appliances at the region level. This means that redundancy and failover rules apply at the region level. You can also set priorities for the server roles that provide failover.

If you have multiple servers in your environment with duplicate failover roles, then you can set the priority of the server role.

- Only server roles that support failover can be marked as primary. These roles only allow one server to be active at a time. These are Notifier, Capacity & Utilization Coordinator, Database Synchronization, Event Monitor, Scheduler, Storage Inventory, and Provider Inventory.

- All other server roles are additive. The more servers with that role in a zone the more work that can be performed.

There are three role priorities.

- Primary: There can only be one primary per zone or region per role. When an appliance is started, the system looks to see if any role is set to primary. If that is the case, the role is activated on that appliance and deactivated from the secondary. In the console, primary roles are shown in bold letters. The text turns red if the server goes down. You must actively set the primary priority.

- Secondary: This is the default priority. There can be multiple secondaries. When an appliance is started, if no primary is found in the zone, the first appliance to start takes the role. In the console, secondary roles are displayed normally with the word "secondary".

- Tertiary: If all appliances with primary roles or secondary roles were down, one of the tertiary would be activated. The reason for tertiary is to ensure that if a server with crucial roles such as Provider Inventory or Event Monitor goes down, you have a way to associate those roles to different appliances by organizing the priorities. Tertiary roles simply show as active in the console.

5.3.2. Region Aware Server Roles

Role	More than one per Region	Can have Priority Set
Automation Engine	Y	N
Database Operations	Y	N
Database Synchronization	N	Y
Notifier	N	Y
Reporting	Y	N
Scheduler	N	Y
User Interface	Y	N
Web Services	Y	N

5.3.3. Setting the Priority of a Failover Role

Procedure 5.40. To Set the Priority of a Failover Role

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Depending on how you want to view your servers, click either the **Roles by Servers** tab or the **Servers by Roles** tab.

4. In the **Status of Roles for Servers in Zone Default Zone** area, click on the role that you want to set the priority for.

5. Click ⚙ (**Configuration**), and ⤴ (**Promote Server**) to make this the primary server for this role.

6. Click ⚙ (**Configuration**), and ⤵ (**Demote Server**) to demote the priority of this server for this role.

5.3.4. Replication

You must be on the server where replication has been set up to check status. To run backups, the database operations server role must be enabled. Databases can then be restored using the black console on the CloudForms Management Engine Appliance. These features are available only when using the internal **PostgreSQL** VMDB.

5.3.4.1. Checking Status of Replication

Procedure 5.41. To Check Status of Replication

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click **Region** name.

3. Click the **Replication** tab.

Result:

If directed to by Red Hat, you may need to reset replication. Do this from the server that is replicating up to a higher level VMDB. When you do this, the subordinate regions data is removed from the top level, and then the replication is restarted.

5.3.4.2. Resetting Replication

Procedure 5.42. To Reset Replication

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click **Region** name.

3. Click the **Replication** tab.

4. Click **Reset**.

5.3.4.3. Running a Single Backup

Procedure 5.43. To Run a Single Backup

1. Navigate to **Configure** → **Configuration**.

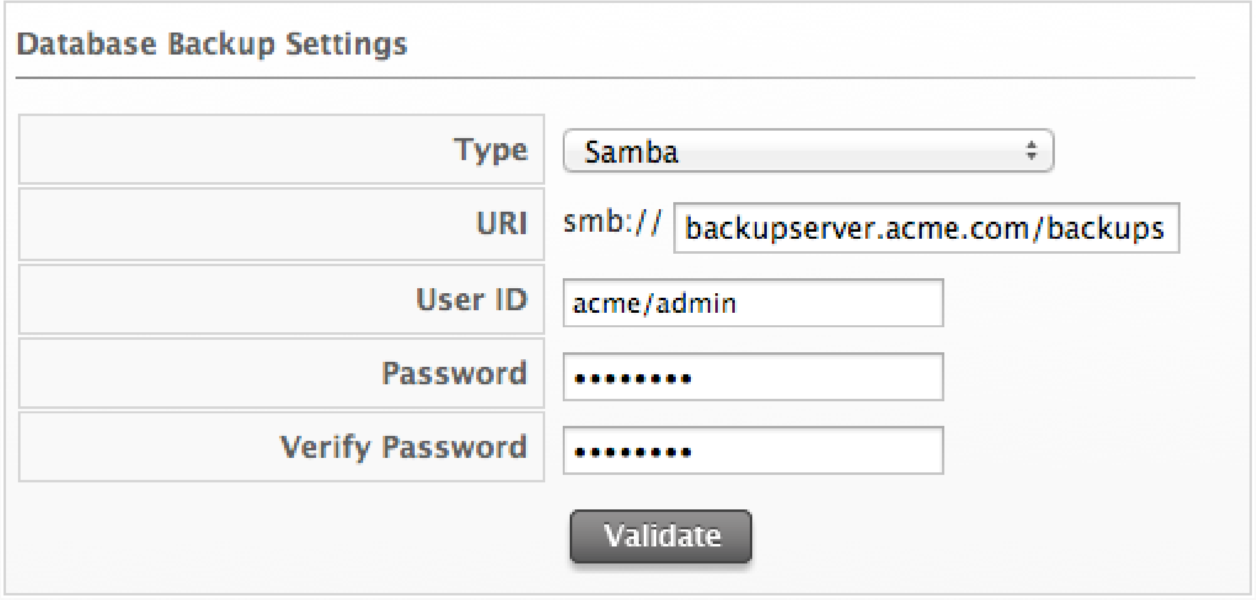
2. Click on the **Diagnostics** accordion, then click **Region** name.

3. Click the **Database** tab.

4. If you have created a backup schedule, and want to use the same depot settings, select it under **Backup Schedules**.

5. If you do not want to use the settings from a backup schedule, or need to create settings, go into the **Database Backup Settings** area.

6. Select a type of server to put the backups. You can either use **Network File System** or **Samba**.



Database Backup Settings

Type	Samba
URI	smb:// backupserver.acme.com/backups
User ID	acme/admin
Password	••••••••
Verify Password	••••••••

   - If selecting **Samba**, enter the **URI**, **User ID**, a **Password**, and a **Verify Password**. Click **Validate** to check the settings.
   - If you choose **Network File System**, enter the **URI**.

7. Click **Submit**.

Result:

The database backup is run immediately. You can see the task by navigating to **Configure** → **Tasks**, then clicking on the **All Other Tasks** tab.

5.3.4.4. Restoring a Database from Backup

Procedure 5.44. To Restore a Database from Backup

1. Copy the database backup file to **/tmp**, and name it **evm_db.backup**. The server looks specifically for this file to restore from.
2. Log in to the black appliance console with a user name of **admin** and the default password. The CloudForms Management Engine Appliance summary screen displays.
3. Press **Enter** to manually configure settings.
4. Press the number **8** to select **Restore Database From Backup**.
5. Press **Y** to confirm.

Result:

If directed by Red Hat, you can run database garbage collection to reclaim unused space in your VMDB. Generally, the database server does this automatically.

5.3.5. Zone Diagnostics

The console provides a way to see all the server roles that a server has been assigned and if these roles are running. This is especially helpful when you have multiple servers with different server roles. For each zone you can also set a central place for all logs to be collected, and collect capacity and utilization data that may be missing.

5.3.5.1. Viewing the Status of Server Roles

Procedure 5.45. To View the Status of Server Roles

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Depending on how you want to view your servers, click either **Roles by Servers** or the **Servers by Roles**.

5.3.5.2. Setting Server Role Priorities

If you have multiple servers in your environment with duplicate failover roles, then you can set the priority of the server role.

- Only server roles that support failover can be marked as primary. These are Notifier, Capacity & Utilization Coordinator, Database Synchronization, Event Monitor, Scheduler, Storage Inventory, and Provider Inventory.
- All other server roles are additive. The more servers with that role in a zone the more work that can be performed.

There are three role priorities.

- Primary: There can only be one primary per zone per role. When an appliance is started, the system looks to see if any role is set to primary. If that is the case, the role is activated on that appliance and deactivated from the secondary. In the console, primary roles are shown in bold letters. The text turns red if the server goes down.
- Secondary: This is the default priority. There can be multiple secondaries. When an appliance is started, if no primary is found in the zone, the first appliance to start takes the role. In the console, secondary roles are displayed normally with the word "secondary".
- Tertiary: If all appliances with primary roles or secondary roles are down, one of the tertiary would be activated. The reason for tertiary is to ensure that if a Server with crucial roles such as Provider Inventory or Event Monitor goes down, you have a way to associate those roles to different appliances by organizing the priorities. Tertiary roles simply show as active in the console.

5.3.5.3. Zone Aware Server Roles

Role	More than one per Zone?	Can have Priority Set
Automation Engine	Y	N
Capacity & Utilization Coordinator	N	Y
Capacity & Utilization Data Collector	Y	N

Role	More than one per Zone?	Can have Priority Set
Capacity & Utilization Data Processor	Y	N
Database Operations	Y	N
Database Synchronization	N	Y
Event Monitor	N	Y
Provider Inventory	N	Y
Provider Operations	Y	N
Notifier	N	Y
Reporting	Y	N
Scheduler	N	Y
SmartProxy	Y	N
SmartState Analysis	Y	N
SmartState Drift Analysis	Y	N
User Interface	Y	N
Web Services	Y	N

5.3.5.4. Setting the Priority of a Failover Role

Procedure 5.46. To Set the Priority of a Failover Role

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Depending on how you want to view your servers, click either the **Roles by Servers** tab or the **Servers by Roles** tab.

4. From the **Status of Roles for Servers in Zone Default Zone** area, click on the role that you want to set the priority for.

5. Click ⤴ **(Promote Server to primary for this role)** to make this the primary Server for this role.

6. Click ⤵ **(Demote Server to normal for this role)** to demote the priority of this Server for this role.

5.3.5.5. Removing an Inactive Server

Procedure 5.47. To Remove an Inactive Server

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Click on the name of the server in the tree view.

4. Click 🗑 (**Delete Server**). This button is available only if the server is inactive.

5.3.5.6. Zone Log Collections

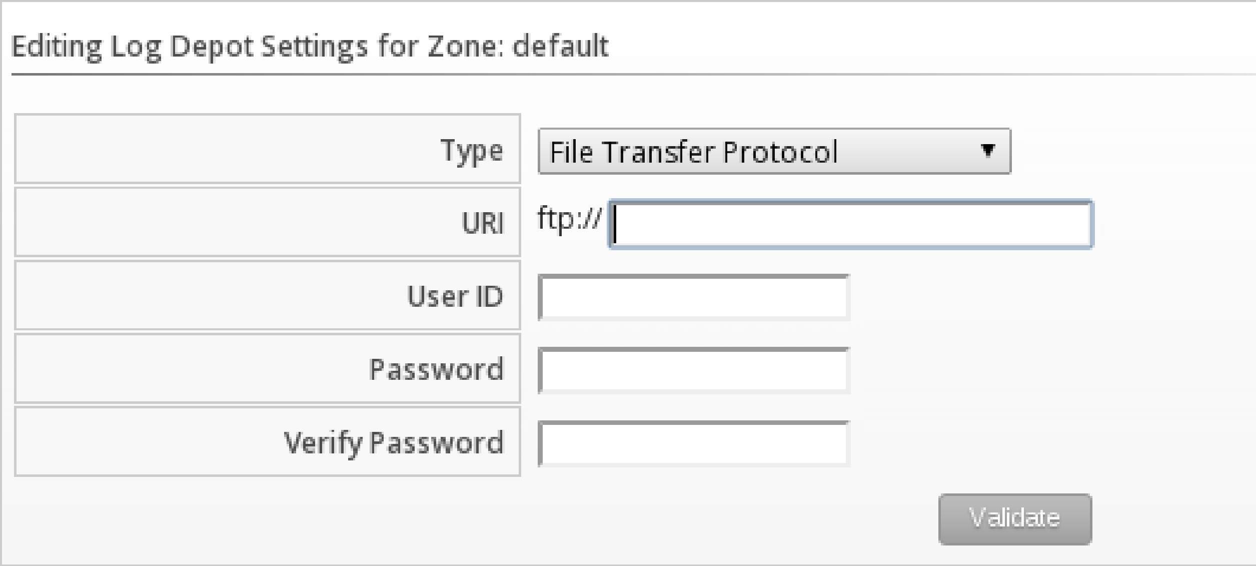
5.3.5.6.1. Zone Log Collection Settings

If you have multiple servers reporting to one central VMDB, then you can collect the configuration files and logs from the console of any of the servers. While you can set this either at the zone or server level, settings at the server level supersede the ones at the zone level. You will designate a log depot which is an File Transfer Protocol, Samba, or Network File System location to store the files. See your network administrator if need to set up one of these shares. You will also need a user that has write access to that location.

5.3.5.6.2. Setting the Location of the Log Depot

Procedure 5.48. To Set the Location of the Log Depot

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Click **Collect Logs**.
4. Click ✎ (**Edit the Log Depot Settings for the selected Zone**).
5. Select the **Type** of share.



Editing Log Depot Settings for Zone: default

Type	File Transfer Protocol ▾
URI	ftp://
User ID	
Password	
Verify Password	

6. Type in the appropriate settings for the **URI**.

> **Note**
>
> Use the fully qualified domain name (FQDN) of the destination server.

7. Type a **Password** and a **Verify Password**.
8. Click **Validate** to check the settings.
9. Click **Save**.

5.3.5.6.3. Collecting and Downloading Logs from All Servers in a Zone

Procedure 5.49. To Collect and Download Logs from all Servers in a Zone

1. Navigate to **Configure** → **Configuration**.
2. Click on the **`Diagnostics`** accordion, then click the **`Zone`** that you want to view.
3. Click the **`Collect Logs`** tab.
4. Click (**`Collect logs`**). All files in the logs directory as well as configuration files are collected.
5. Click **`OK`**. The status of the log retrieval shows in the CloudForms Management Engine console.

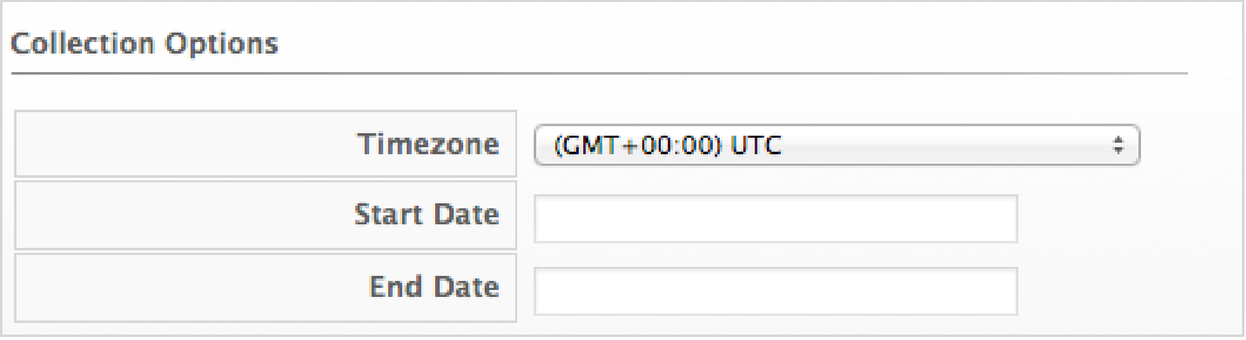
5.3.5.7. Capacity and Utilization Repair

Under certain circumstances, it is possible that CloudForms Management Engine is not able to collect capacity and utilization data. This could be due to password expiration, a change in rights to the cloud provider and this change didn't provide enough granularity to the CloudForms Management Engine service account, or network connectivity. The gap data is collected directly by extracting the monthly performance data. Gap collection need to be completed for each zone individually. Therefore, the procedure below need to be repeated for each zone.

5.3.5.7.1. Repairing Capacity and Utilization Data

Procedure 5.50. To Repair Capacity and Utilization Data

1. Login to a CloudForms Management Engine Appliance located in the zone for which you want to gather the data.
2. Navigate to **Configure** → **Configuration**.
3. Click on the **`Diagnostics`** accordion, then click the **`Zone`** that you want to view.
4. Click **`C & U Gap Collection`**.



Collection Options

Timezone	(GMT+00:00) UTC
Start Date	
End Date	

   - Select the appropriate **`Timezone`**.
   - *Do not select more than one week unless instructed to do so by Red Hat Support.*
   - Select a **`Start Date`**.
   - Select an **`End Date`**.

5. Click **`Submit`**.

Result:

After the gap collection has completed for this zone, repeat these same steps for the next zone. You can check for completion by going to the clusters page and checking for the capacity and utilization data for the time period specified.

5.3.6. Server Diagnostics

Under Diagnostics for a server, you can view the status of CloudForms Management Engine workers running on the server, set log collection setting for only that server, and view the server's current CloudForms Management Engine and audit logs.

5.3.6.1. Workers

The **Workers** tab enables you to see the status of and restart CloudForms Management Engine Workers.

You can see additional information on and restart the following items.

- C & U Metrics Collectors that collects capacity and utilization data.
- C & U Metrics Processors, which processes the collected capacity and utilization data.
- Database Replication Worker that is responsible for maintaining replication activities.
- Event Handlers put events from the Event Monitor into the VMDB and starts CloudForms Management Engine processes if needed base on that information.
- Event Monitors that communicate with the external cloud provider to deliver up to date event information.
- Generic Workers that perform long running and priority processes.
- Priority Workers that perform high priority, short processes.
- Schedule Workers that maintains any items that run on a schedule.
- Session Broker that maintains a single connection to the cloud providers .
- Refresh Workers that runs the refresh processes.
- Reporting Workers that generate reports.
- SmartProxy Workers that run SmartState Analyses on virtual machine.
- User Interface Worker that allows users access to the console.
- Web Services Worker that maintains CloudForms Management Engine Web services.
- VM Analysis Collectors that run and process SmartState Analyses on virtual machines.

5.3.6.1.1. Reloading Worker Display

Procedure 5.51. To Reload Worker Display

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Select the server that you want to view.

4. Click the **Workers** tab.

5. Click ↻ (**Refresh Current Workers display**).

5.3.6.1.2. Restarting a CloudForms Management Engine Worker

Procedure 5.52. To Restart a CloudForms Management Engine Worker

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to view.

4. Click on the **Workers** tab.

5. Click on the worker you want to restart.

6. Click ▶ (**Restart selected worker**).

7. Click **OK** to confirm.

5.3.6.2. Server and Audit Logs

5.3.6.2.1. Collecting Server Logs and Configuration Files

While you can designate a central location to collect logs for all servers in a specific zone, you can override those values for a specific server. To do this, designate a log depot which is an File Transfer Protocol, Samba, or Network File System location to store the files. See your network administrator to set up one of these shares. You also need a user that has write access to that location. Settings at the server level supersede the ones at the zone level.

5.3.6.2.2. Setting the Location of the Log Depot for a Specific Server

Procedure 5.53. To Set the Location of the Log Depot for a Specific Server

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to collect logs for.

4. Click on the **Collect Logs** tab.

5. Click ✏ (**Edit Log Depot Settings for the selected Server**).

6. Select the **Type** of share.

7. Type in the appropriate settings for the **URI**.

> **Note**
>
> Use the fully qualified domain name (FQDN) of the destination server.

8. Click **Validate** to check the settings.

9. Click **Save**.

5.3.6.2.3. Collecting the Current Log Set of a Server

Procedure 5.54. To Collect the Current Log Set of a Server

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to collect logs for.

4. Click on the **Collect Logs** tab.

5. Click (**Collect**), then click (**Collect current logs**). All current log files in as well as configuration files are collected.

6. Click **OK**. The status of the log retrieval shows in the CloudForms Management Engine console.

5.3.6.2.4. Collecting All Log Sets from a Server

Procedure 5.55. To Collect All Log Sets from a Server

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to collect logs for.

4. Click **Collect Logs**.

5. Click (**Collect**), then click (**Collect all logs**). All files in the logs directory as well as configuration files are collected.

6. Click **OK**. The status of the log retrieval shows in the CloudForms Management Engine console.

5.3.6.2.5. Viewing the Server, Audit, and Production Logs

The server and audit logs roll over daily. The previous logs are stored as zipped files in the **/var/www/miq/vmdb/log** folder. The current logs can be easily viewed and downloaded from the **Configure** → **Configuration**, then click on the **Diagnostics** accordion.

Use the server log to see all actions taken by the server including communication with the SmartProxy and tasks.

5.3.6.2.6. Viewing the Server Log

Procedure 5.56. To View the Server Log

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to view.

4. Click **CFME Log**.

The CloudForms Management Engine server automatically retrieves the last 1000 lines of the log.

5.3.6.2.7. Reloading the Server Log

Procedure 5.57. To Reload the Server Log

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to view.

4. Click **CFME Log**.

5. Click ↻ (**Reload the Log Display**).

5.3.6.2.8. Downloading the Server Log

Procedure 5.58. To Download the Server Log

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to view.

4. Click **CFME Log**.

5. Click ⬇ (**Download the Entire Log File**).

Note

Use the Audit Log to see changes to the user interface and authentication.

5.3.6.2.9. Viewing the Audit Log

Procedure 5.59. To View the Audit Log

1. Navigate to **Configure** → **Configuration**.

2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.

3. Select the server that you want to view.

4. Click **Audit Log**.

Result:

The server automatically retrieves the last 1000 lines of the log.

5.3.6.2.10. Reloading the Audit Log

Procedure 5.60. To Reload the Audit Log

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Select the server that you want to view.
4. Click **Audit Log**.
5. Click ↻ (**Reload the Audit Log Display**).

5.3.6.2.11. Downloading the Audit Log

Procedure 5.61. To Download the Audit Log

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Select the server that you want to view.
4. Click **Audit Log**.
5. Click ⬇ (**Download the Entire Audit Log File**).

5.3.6.2.12. Viewing the Production Log

Use the production log to see all actions performed using the console.

Procedure 5.62. To View the Production Log

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Select the server that you want to view.
4. Click **Production Log**.

Result:

The CloudForms Management Engine server automatically retrieves the last 1000 lines of the log.

5.3.6.2.13. Reloading the Production Log

Procedure 5.63. To Reload the Production Log

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Click **Production Log**.
4. Click the **CloudForms Management Engine Log** tab.

5. Click ↻ (**Reload the Product Log Display**).

5.3.6.2.14. Downloading the Production Log

Procedure 5.64. To Download the Production Log

1. Navigate to **Configure** → **Configuration**.
2. Click on the **Diagnostics** accordion, then click the **Zone** that you want to view.
3. Select the server that you want to view.
4. Click **Production Log**.
5. Click ⇩ **(Download the Production Log File)**.

5.4. Database Operations

5.4.1. Viewing Information on the VMDB

The **Database** accordion displays a summary of VMDB information, a list of all tables and indexes, settings for the tables, active client connection, and database utilization.

Procedure 5.65. To View Information on the VMDB

1. Navigate to **Configure** → **Configuration**.
2. Click the **Database** accordion.
3. Click **VMDB** in the tree view on the left.
4. Click the appropriate tab to view the desired information:
   - **Summary**: displays statistics about the database.
   - **Tables**: displays a clickable list of all the tables.
   - **Indexes**: displays a clickable list of all the indexes.
   - **Settings**: displays a list of all tables, their descriptions, and other valuable Information.
   - **Client Connections**: displays all current connections to the VMDB.
   - **Utilization**: displays usage charges for the disk and index nodes.

5.4.2. Database Regions and Replication

5.4.2.1. Database Regions and Replication

Regions are used to create a central database for reporting and charting. Do not use the database at the top level for operational tasks such as SmartState Analysis or Capacity and Utilization data collection. Assign each server participating in the Region a unique number during the regionalization process. After creating the top level region, create the subordinate regions and set each to replicate to the top region. Note that the subordinate regions are not aware of each other from a database perspective. That is, you cannot see information from one subordinate region in another. The only VMDB with visibility to all subordinate regions is the top level.

The following is an example of regionalized database scenario:

1. Create Region Number 99 to which all other VMDBs replicate.

   - Treat this as a read only database for reporting and charting.

   - Enable only the Reporting, Scheduler, and User Interface Server Roles. To perform database maintenance items, such as scheduled backups, on the top-level region (master), also enable the Database Operations role.

   - No additional settings aside from assigning the region ID. No need to configure any replication.

2. Create Region Number 1

   a. Add replication worker settings pointing to the VMDB for Region 99.

   b. Enable Database Synchronization Server role on one Server in the Region. If you have a second Server in the same region, do not enable the DB Synchronization role. Do not enable more than one Database Synchronization Role per Region.

3. Create Region Number 2

   a. Add replication worker settings pointing to the VMDB for Region 99.

   b. Enable Database Synchronization Server role on one Server in the Region. If you have a second Server in the same region, do not enable the DB Synchronization role. Do not enable more than one Database Synchronization Role per Region.

5.4.2.2. Creating a Region

The process of creating a region takes a few minutes. The database is dropped and rebuilt to accommodate the region numbers. After creating a region, upload a valid license file to the VMDB.

Procedure 5.66. To Create a Region

1. Start the appliance and log in to the black appliance console with a user name of ***admin*** and the default password. The **Appliance Summary Screen** displays.

2. Press **Enter** to manually configure settings.

3. Enter **11** to **Stop Server Processes**.

4. Enter **Y** to confirm.

5. After all processes are stopped, press **Enter** to return to the menu.

6. Press **Enter** again to manually configure settings.

7. Enter **9** to select **Setup Database Region**.

> **Warning**
>
> Performing this action destroys any existing data and cannot be undone. Back up the existing database before proceeding. By default, new CloudForms Management Engine Appliances are assigned region 0. Do not use this number when creating a region as duplicating region numbers can compromise the integrity of the data.

8. Enter **Y** to confirm the selection.

9. Enter a database region number that has not been used in your environment. Do not enter duplicate region numbers as this can corrupt the data.

10. Press **Enter**.

11. After the process is complete, press **Enter** to return to the menu.

12. Press **Enter** again to manually configure settings.

13. Enter **12** to select **Start Server Processes**.

14. Enter **Y** to confirm.

Result:

After a region is created, you can create subordinate regions as necessary and set up replication to the top level region.

5.4.2.3. Replicating a Database

Procedure 5.67. To Replicate a Database

1. Navigate to **Configure** → **Configuration**.

2. Click the **Settings** accordion and click **Zones**.

3. Click the **Zone** where the server is located and click the server name.

4. Click **Workers**.

5. In the **Replication Worker** area, enter the worker information:

   a. **Database**: the name of your VMDB.

   b. **Username**: the user name to connect to the VMDB user name.

   c. **Password** and **Verify Password**: the password for the user name.

   d. **Host**: the IP address or hostname of the top level VMDB.

6. Click **Validate** to confirm that the VMDB is accessible.

7. Click **Save**.

5.4.2.4. Enabling the Database Synchronization Role

When you start the replication worker, all of the information in the subordinate database is sent to the top region (99). The worker also creates triggers so that future changes made to subordinate regions are sent automatically to the top region.

Procedure 5.68. To Enable the Database Synchronization Role

1. Navigate to **Configure** → **Configuration**.

2. Click the **Settings** accordion and click **Zones**.

3. Click the **Zone** where the server is located and click the server name.

> **Note**
>
> Only enable database synchronization on subordinate servers with replication worker settings already configured. Do not enable more than one Database Synchronization role per region.

4. Click **Server**.

5. In the **Server Control** area, check **Database Synchronization**.

6. Click **Save**.

5.4.2.5. Scheduling a Database Backup

Schedule database backups on a regular basis to preserve data.

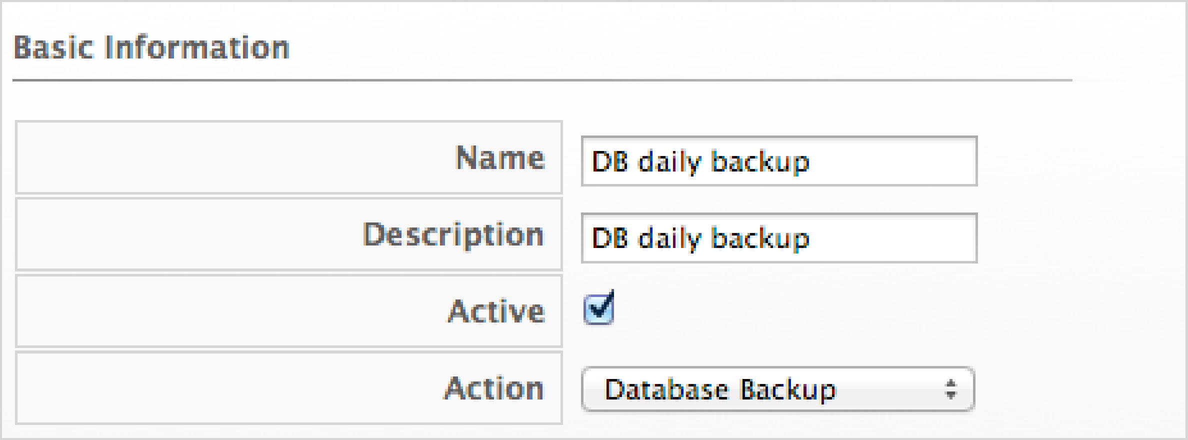
Procedure 5.69. To Schedule a Database Backup

1. Navigate to **Configure** → **Configuration**.

2. Click the **Settings** accordion and click **Schedules**.

3. Click ⚙ (**Configuration**), and ✚ (**Add a new Schedule**).

4. In the **Basic Information** box, enter a **Name** and **Description** for the schedule.



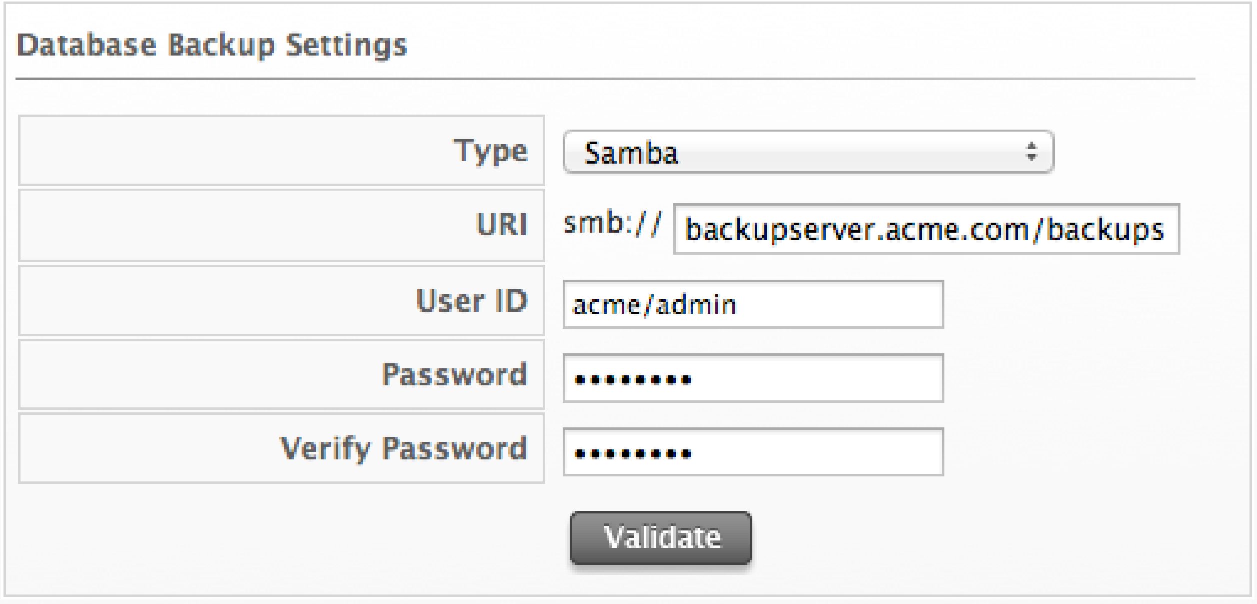
Basic Information

Name	DB daily backup
Description	DB daily backup
Active	☑
Action	Database Backup

5. Check **Active** to enable the backup schedule.

6. In the **Action** drop-down list, select **Database Backup**.

7. In the **Database Backup Settings** box, select a type of server for storing the backups from the **Type** drop-down list. You can use Network File System (NFS) or Samba.

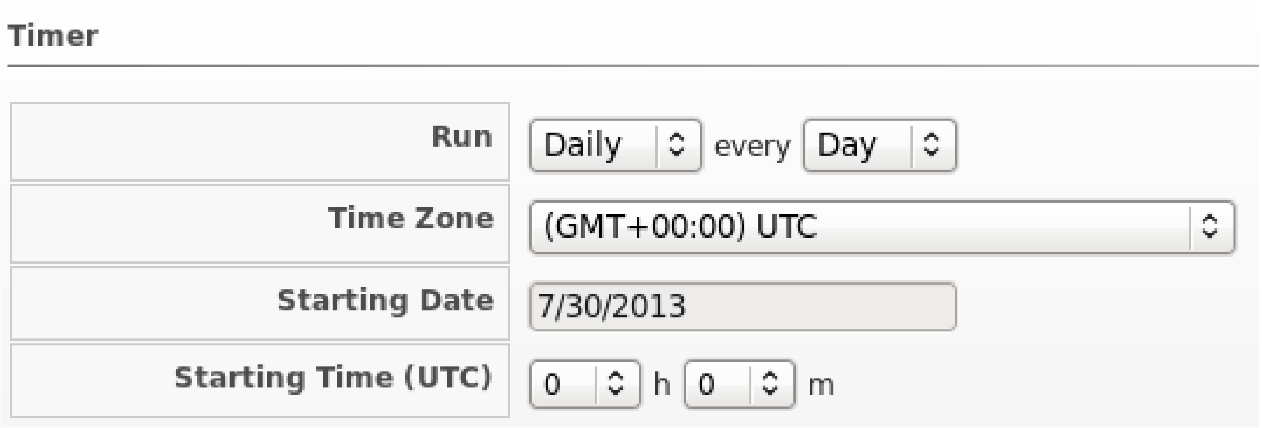


Database Backup Settings

Type	Samba
URI	smb:// backupserver.acme.com/backups
User ID	acme/admin
Password	••••••••
Verify Password	••••••••

- If you select Samba, enter the **URI**, **User ID**, and a valid **Password**. Click **Validate** to check the settings.
- If you select Network File System, enter the **URI**.

8. In the **Timer** box, select the desired backup frequency from the **Run** dropdown list.



Timer

Run	Daily every Day
Time Zone	(GMT+00:00) UTC
Starting Date	7/30/2013
Starting Time (UTC)	0 h 0 m

- Once: the backup runs one time.
- Hourly: select the number of hours between backups from the drop-down list.
- Daily: select the number of days between backups from the drop-down list.
- Weekly: select the number of weeks between backups from the drop-down list.
- Monthly: select the number of months between backups from the drop-down list.

9. Select a **Time Zone** for the schedule.
10. Type or select a **Starting Date** for the schedule.
11. Select a **Starting Time** based on a 24 hour clock.
12. Click **Add**.

5.4.2.6. Running a Single Database Backup

Procedure 5.70. To Run a Single Database Backup

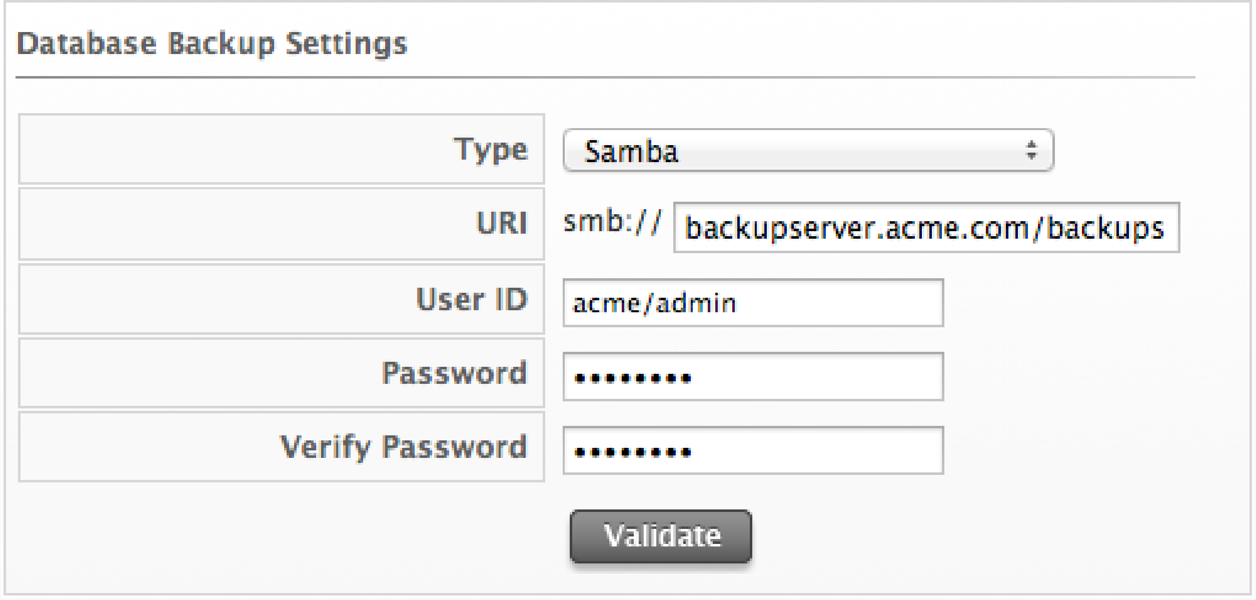
1. Navigate to **Configure** → **Configuration**.

2. Click the **Diagnostics** accordion and click the **Region** name.

3. Click the **Database** tab.

4. If you have created a backup schedule and want to use the same depot settings, select the schedule in the **Backup Schedules** box.

5. If you do not want to use the settings from a backup schedule, select a type of server for storing the backups from the **Type** drop-down list in the **Database Backup Settings** box. You can use Network File System (NFS) or Samba.



Database Backup Settings

Type	Samba
URI	smb:// backupserver.acme.com/backups
User ID	acme/admin
Password	••••••••
Verify Password	••••••••

- If you select Samba, enter the **URI**, **User ID**, and a valid **Password**. Click **Validate** to check the settings.

- If you select Network File System, enter the **URI**.

6. Click **Submit** to run the database backup.

5.4.2.7. Restoring a Database from a Backup

If a database is corrupt or fails, restore it from a backup.

Procedure 5.71. To Restore a Database from a Backup

1. Save the database backup file as **/tmp/evm_db.backup**. CloudForms Management Engine looks specifically for this file when restoring a database from a backup.

2. Log in to the black appliance console with a user name of ***admin*** and the default password. The **Appliance Summary Screen** displays.

3. Press **Enter** to manually configure settings.

4. Enter **11** to **Stop Server Processes**. Stop the process on all servers that connect to this VMDB.

5. Enter **Y** to confirm.
6. After all processes are stopped, press **Enter** to return to the menu.
7. Press **Enter** again to manually configure settings.
8. Enter **8** to select **Restore Database From Backup**. If connections are open, the server may still be shutting down. Wait a minute and try again.
9. Enter **y** to keep the database backup after restoring from it. Enter **n** to delete it.
10. Press **Y** to confirm.
11. After the backup completes, press **Enter** to return to the menu.
12. Press **Enter** again to manually configure settings.
13. Enter **12** to **Start Server Processes**.
14. Enter **Y** to confirm.

5.4.2.8. Running Database Garbage Collection

The database server collects garbage automatically, but Red Hat may occasionally direct you to run database garbage collection manually in order to reclaim unused space in your VMDB.

Procedure 5.72. To Run Database Garbage Collection

1. Navigate to **Configure** → **Configuration**.
2. Click the **Diagnostics** accordion and click the **Region** name.
3. Click the **Database** tab.
4. In the **Run Database Garbage Collection Now** box, click **Submit**.

Chapter 6. SmartProxies

The embedded SmartProxy can analyze virtual machines that are registered to a host and templates that are associated with a provider. To provide visibility to repositories, install the SmartProxy on a host from the console. This SmartProxy can also analyze virtual machines on the host on which it is installed.

6.1. Installing the SmartProxy from the Console

The server comes with one SmartProxy version already available. It can also be installed on an ESX Server version 3.0.2, 3.5 or 4.

> **Important**
>
> Contact Red Hat before installing a new SmartProxy on an ESX Server.

Requirements:

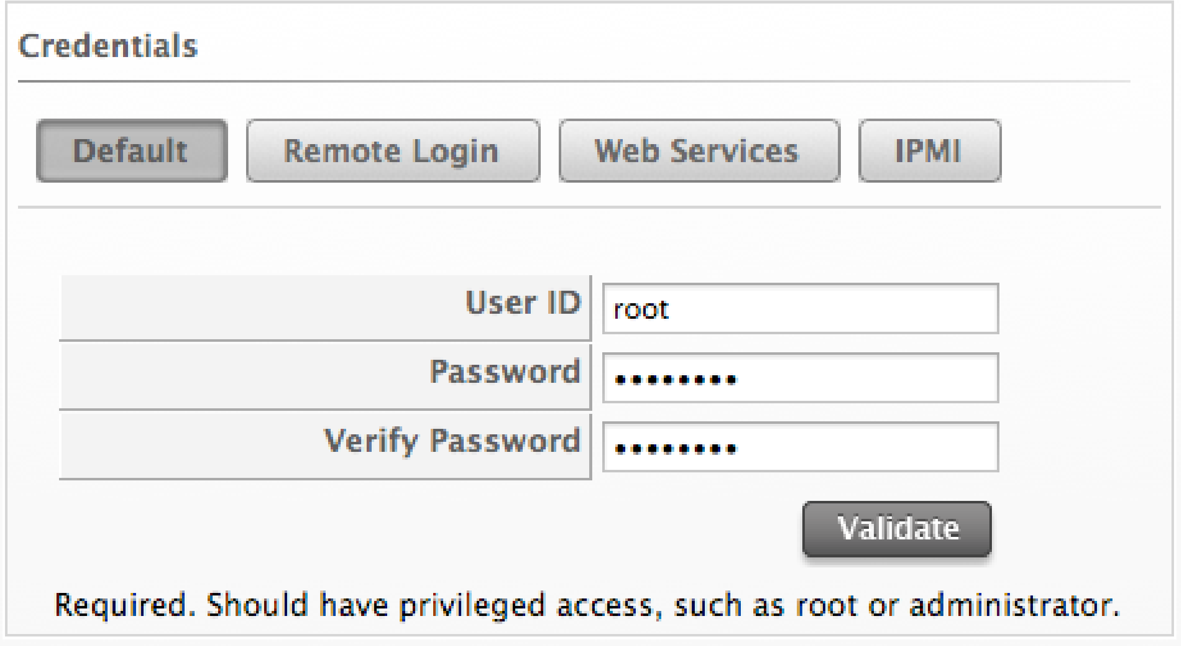
- On ESX, SSH (Secure Shell) must be enabled. This is usually port 22.
- 300 MB free disk space to install and run the SmartProxy.
- Administrator or root credentials.
- The host must already be in the VMDB either by discovery or manually. See the *Insight Guide* for information on discovery.

6.2. Entering Credentials and Operating System for the Target Host

Set the credentials and operating system for the target host to prepare for the installation of SmartProxy.

Procedure 6.1. To Enter Credentials and Operating System for the Target Host

1. Navigate to **Infrastructure** → **Hosts**.
2. Check the host you want to edit.
3. Click ⚙ (**`Configuration`**), then ✎ (**`Edit Selected Hosts`**).
4. In the **`Credentials`** box, click the **`Default`** tab and enter your login credentials. If you are using domain credentials, the format for **`User ID`** must be in the format of *<domainname>**<username>*. For ESX hosts, if SSH login is disabled for the default user, click the **`Remote Login`** tab and enter a user with remote login access.



User ID: root

Password: •••••••••

Verify Password: •••••••••

Required. Should have privileged access, such as root or administrator.

> **Important**
>
> If the target is a Windows host, disconnect all network connections between the Windows proxy and the target. If an existing connection uses a different set of credentials than those set in the console, the installation may fail.

5. Click **Validate** to verify the credentials.

6. If you added the host manually instead of **Host Discovery** or **Provider Refresh** finding it, select the host's operating system from the **Host Platform** drop-down box to ensure the host platform is available.

7. Click **Save**.

When remotely installing on Windows hosts, the SmartProxy file is first copied to a Windows proxy. That computer then installs the file to the target host. The Windows proxy is the same as when you check the **Default Repository SmartProxy** box located by navigating to **Configure** → **Configuration**, then clicking on the desired server, then the **Server** tab, and exploring the **Server Control** area.

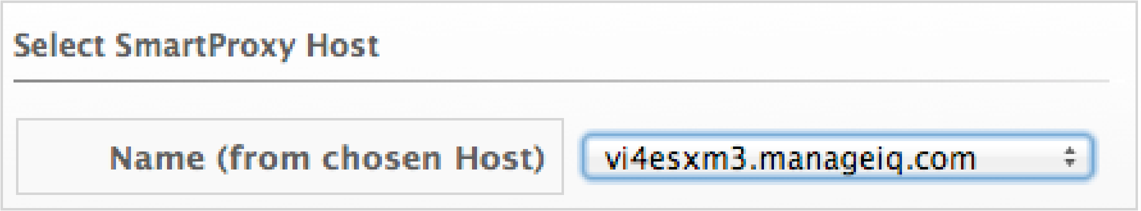
6.3. Adding a SmartProxy

Procedure 6.2. To Add a SmartProxy

1. Navigate to **Configure** → **Smartproxies**.

2. Click + (**Add a new SmartProxy**).

3. From the **Name** dropdown, select the host on which you want to install the SmartProxy.



Select SmartProxy Host

Name (from chosen Host): vi4esxm3.manageiq.com

4. Click **Add**.

6.4. Installing a SmartProxy

Procedure 6.3. To Install a SmartProxy

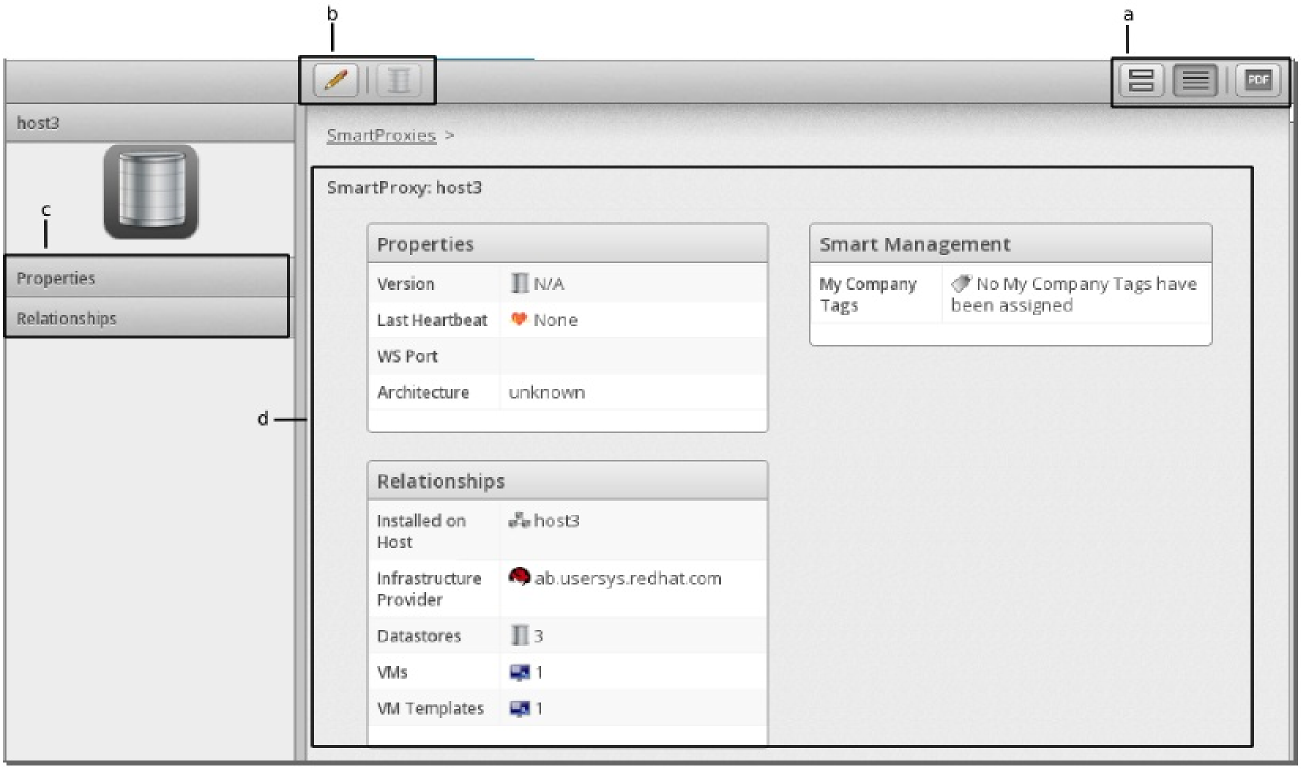
1. Navigate to **Configure** → **Smartproxies**.
2. Check the SmartProxy where you want to install the software.
3. Click (**`Deploy to the selected SmartProxy`**).
4. From **`Version to Install`**, select the version of the SmartProxy to install.
5. If you have already entered credentials for this host, the **`Credentials`** area should already be entered. Otherwise, on the Credentials, Default tab type a user name with elevated security credentials and the users password. If you are using domain credentials, the format for User ID must be in the format of <domainname>\<username>. On ESX hosts, if SSH login is disabled for the Default user, type in a user with remote login access on the Remote Login tab. See *Editing Host Information*.
6. Click **`Validate`** to verify the credentials.
7. Click **Save**.

6.5. Reviewing a SmartProxy

6.5.1. Reviewing a SmartProxy

After viewing your list of SmartProxies, you can review a specific SmartProxy by clicking on it. The screen provides you with a SmartProxy taskbar, a SmartProxy accordion, and a SmartProxy summary.

- Use the SmartProxy taskbar to modify the SmartProxy settings.
- Use the SmartProxy accordion to view the log and summary of the SmartProxy.
- Use the SmartProxy summary to drill down to the SmartProxy relationships.



host3

Properties

Relationships

SmartProxies >

SmartProxy: host3

Properties	
Version	N/A
Last Heartbeat	None
WS Port	
Architecture	unknown

Smart Management	
My Company Tags	No My Company Tags have been assigned

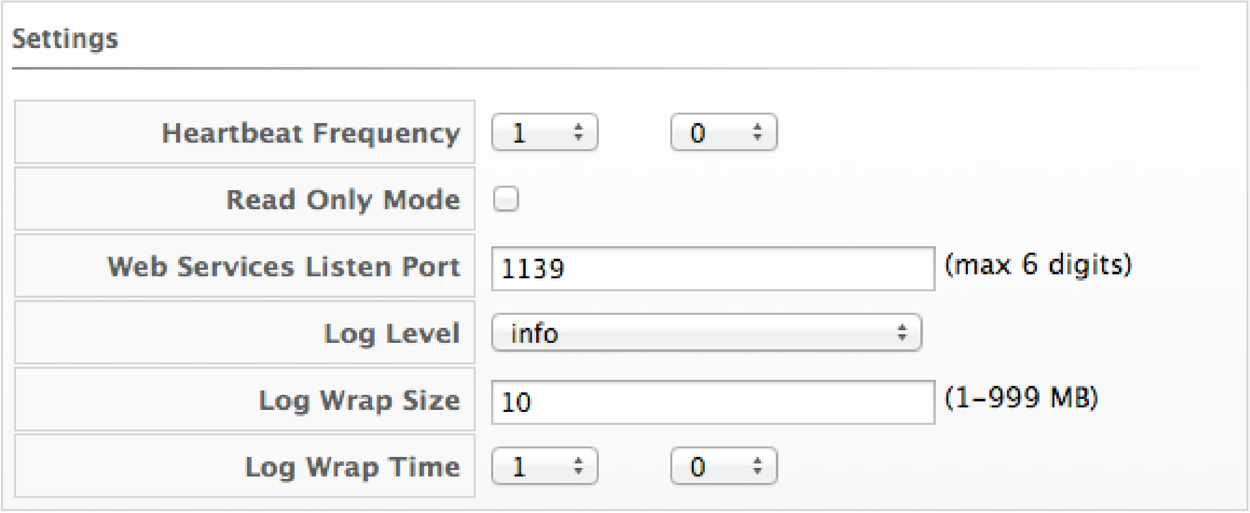
Relationships	
Installed on Host	host3
Infrastructure Provider	ab.usersys.redhat.com
Datastores	3
VMs	1
VM Templates	1

1. SmartProxy Views
2. SmartProxy Taskbar
3. SmartProxy Accordion
4. SmartProxy Summary

6.5.2. Editing SmartProxy Settings

Procedure 6.4. To Edit SmartProxy Settings

1. Navigate to **Configure** → **Smartproxies**.
2. Click the SmartProxy that you want to edit.
3. From the SmartProxy Taskbar, click (**`Edit this SmartProxy`**).



Settings

Heartbeat Frequency	1	0
Read Only Mode	□	
Web Services Listen Port	1139	(max 6 digits)
Log Level	info	
Log Wrap Size	10	(1-999 MB)
Log Wrap Time	1	0

- Use **Heartbeat Frequency** to configure how often you want the SmartProxy to contact the CloudForms Management Engine Appliance to check for tasks.

- Check **Read Only Mode** so that the SmartProxy will not perform any tasks that change the host computer or virtual machines. For example, the SmartProxy will discover and analyze, but will not stop, start, or pause virtual machines.

- Use **Web Services Listen Port** to specify the port you want web services for the SmartProxy to listen on.

- Use **Log Level** to specify the default log level for the SmartProxy log.

- Use **Log Wrap Size** to set a size for the log to wrap in megabytes. The size can be from 1 to 999 MB.

- Use **Log Wrap Time** to set a time frequency for log wrapping.

> **Note**
>
> Log wrapping occurs on whichever limit is reached first, size or time.

4. Modify settings for this specific SmartProxy.

5. Click **Save** to activate the changes. Click **Reset** to undo any changes you made on the current session of this page.

6.5.3. Updating the SmartProxy

Procedure 6.5. To Update the SmartProxy

1. Navigate to **Configure** → **Smartproxies**.

2. Click the SmartProxy that you want to update.

3. Click (**Re-install over the SmartProxy version on the Host**).

4. From **Version to Install**, select the new version of the SmartProxy to install.

5. If you have already entered credentials for this host, the **Credentials** area should already be completed. Otherwise, on the **Credentials Default** tab type a user

name with elevated security credentials and the users password. If you are using domain credentials, the format for User ID must be in the format of <domainname>\<username>. On ESX hosts, if SSH login is disabled for the Default user, type in a user with remote login access on the Remote Login tab. See *Editing Host Information*.

6. Click **Validate** to verify the credentials.
7. Click **Save**.

6.6. SmartProxy Accordion

6.6.1. SmartProxy Accordion

Use the SmartProxy Accordion to view the summary of the SmartProxy, view its logs, and view the objects it is related to.

- Click Properties to view the SmartProxy Summary screen and the SmartProxy logs.
- Click Relationships to see the items related to this SmartProxy.

6.6.2. Viewing the SmartProxy Summary

Use the **Server Summary** to see the member virtual machines.

Procedure 6.6. To View the SmartProxy Summary

1. Navigate to **Configure** → **Smartproxies**.
2. Click the SmartProxy that you want to view. The summary is automatically displayed.
3. If you have navigated away from the summary, click **Properties**, then **Summary**.

6.6.3. Viewing the SmartProxy Log

Use the logs to troubleshoot communications and operational events of the SmartProxy. The server gets the log on demand.

Procedure 6.7. To View the SmartProxy Log

1. Navigate to **Configure** → **Smartproxies**.
2. Click the SmartProxy with the log you want to view.
3. From the **SmartProxy** accordion, click **Properties**, and then **Log Viewer**.
4. Click 🔄 (**Retrieve the current SmartProxy log**) to get the latest log from the SmartProxy.
5. Refresh your browser.

6.6.4. Downloading the SmartProxy Log

This procedure decsribes how to download a SmartProxy log.

Procedure 6.8. To Download the SmartProxy Log

1. Navigate to **Configure** → **Smartproxies**.
2. Click the SmartProxy with the log you want to download.
3. From the **`SmartProxy`** accordion, click **`Properties`**, and then **`Log Viewer`**.
4. Click ⬇ (**`Download the SmartProxy log as a Zip File`**) to download the log.

Chapter 7. About

7.1. Accessing CloudForms Management Engine Guides and Support

In the **About** area of **Configure**, you can see session information for the console, download PDFs of the CloudForms Management Engine documentation and navigate to the Red Hat Customer Portal site.

Procedure 7.1. To View Session Information, Documentation, and the Red Hat Customer Portal Link

1. Navigate to **Configure** → **About**.
2. To go to the Red Hat Customer Portal, click the link to http://access.redhat.com/home.
3. To view the documentation, click the document title.

Revision History

Revision 0.0.0-2	**Tue Sep 2 2014**	**CloudForms Docs Team**

Initial book creation.