CloudForms 3.1
Management Engine 5.3 Control Guide

Policy-based Enforcement, Compliance, Alerting

Red Hat CloudForms Documentation Team

CloudForms 3.1 Management Engine 5.3 Control Guide

Policy-based Enforcement, Compliance, Alerting

Red Hat CloudForms Documentation Team

Legal Notice

Abstract

This guide provides instructions for policy-based actions in a CloudForms Management Engine environment, including system controls, enforcement, compliance, and alerts. 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.

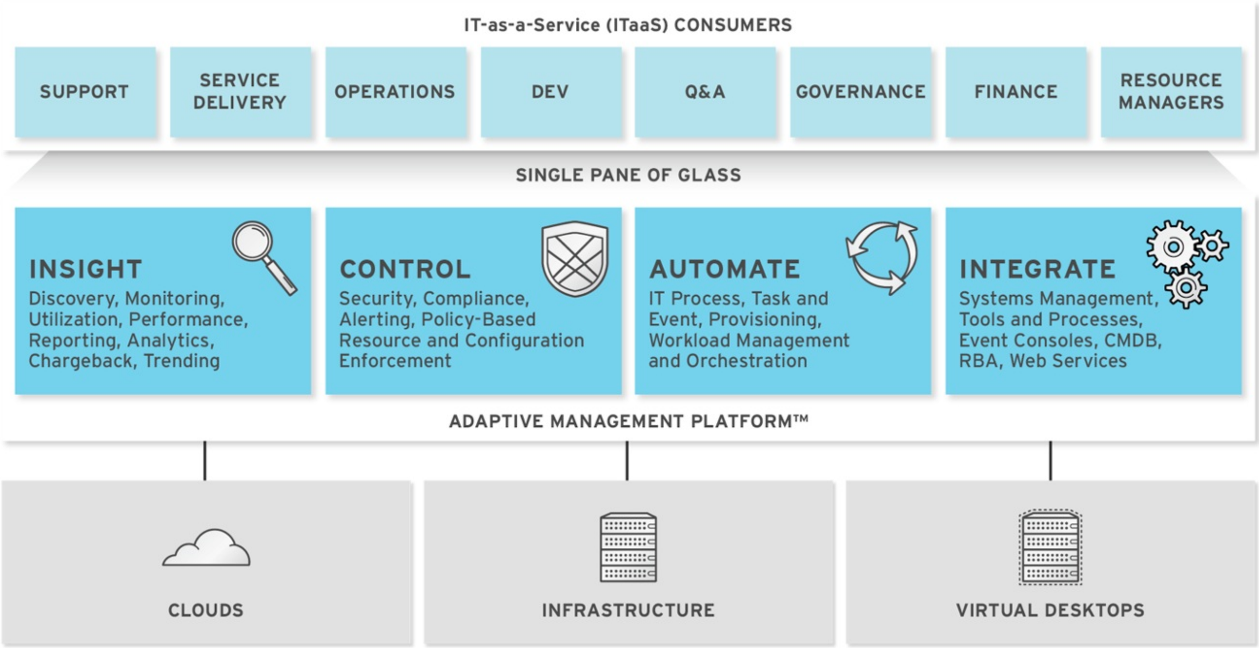

IT-as-a-Service (ITaaS) CONSUMERS
SUPPORT
SERVICE DELIVERY
OPERATIONS
DEV
Q&A
GOVERNANCE
FINANCE
RESOURCE MANAGERS
SINGLE PANE OF GLASS
INSIGHT
Discovery, Monitoring, Utilization, Performance, Reporting, Analytics, Chargeback, Trending
CONTROL
Security, Compliance, Alerting, Policy-Based Resource and 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.

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: *Control 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. Policies

Policies are used to manage your virtual environment. There are two types of policies available: compliance and control. Compliance policies are used to harden your virtual infrastructure, making sure that your security requirements are adhered to. Control policies are used to check for a specific condition and perform an action based on the outcome. For example:

- Prevent virtual machines from running without an administrator account.
- Prevent virtual machines from starting if certain patches are not applied.
- Configure the behavior of a production virtual machine to only start if it is running on a production host.
- Force a SmartState Analysis when a host is added or removed from a cluster.

2.1. Control Policies

A control policy is a combination of an event, a condition, and an action. This combination provides management capabilities in your virtual environment.

- An event is a trigger to check a condition.
- A condition is a test triggered by an event.
- An action is an execution that occurs if a condition is met.

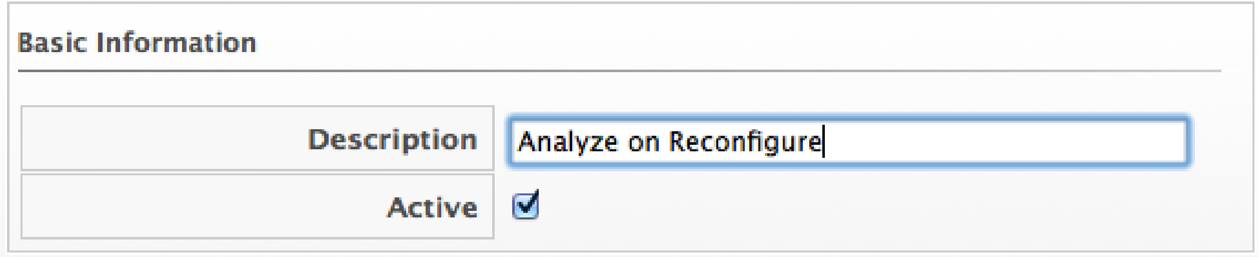
2.1.1. Creating Control Policies

Create control policies by combining an event, a condition, and an action. Plan carefully the purpose of your policy before creating it. You can also use a scope expression that is tested immediately when the policy is triggered by an event. If the item is out of scope, then the policy does not continue on to the conditions, and none of the associated actions run.

The procedure below describes how to create a control policy, its underlying conditions, and assign its events and actions in one process. Conditions and custom actions can be created separately as well. Those procedures are described in later sections in conditions and actions. Also, a description of all events is provided in events.

Procedure 2.1. To Create a Control Policy

1. Navigate to **Control** → **Explorer**.
2. Click the **Policies** accordion, and select **`Control Policies`**.
3. Select either **Host Control Policies** or **VM Control Policies**.
4. Click ⚙ (**`Configuration`**), + (**`Add a New Control Host/Vm Policy`**).
5. Type in a **`Description`**.



Basic Information

Description: Analyze on Reconfigure

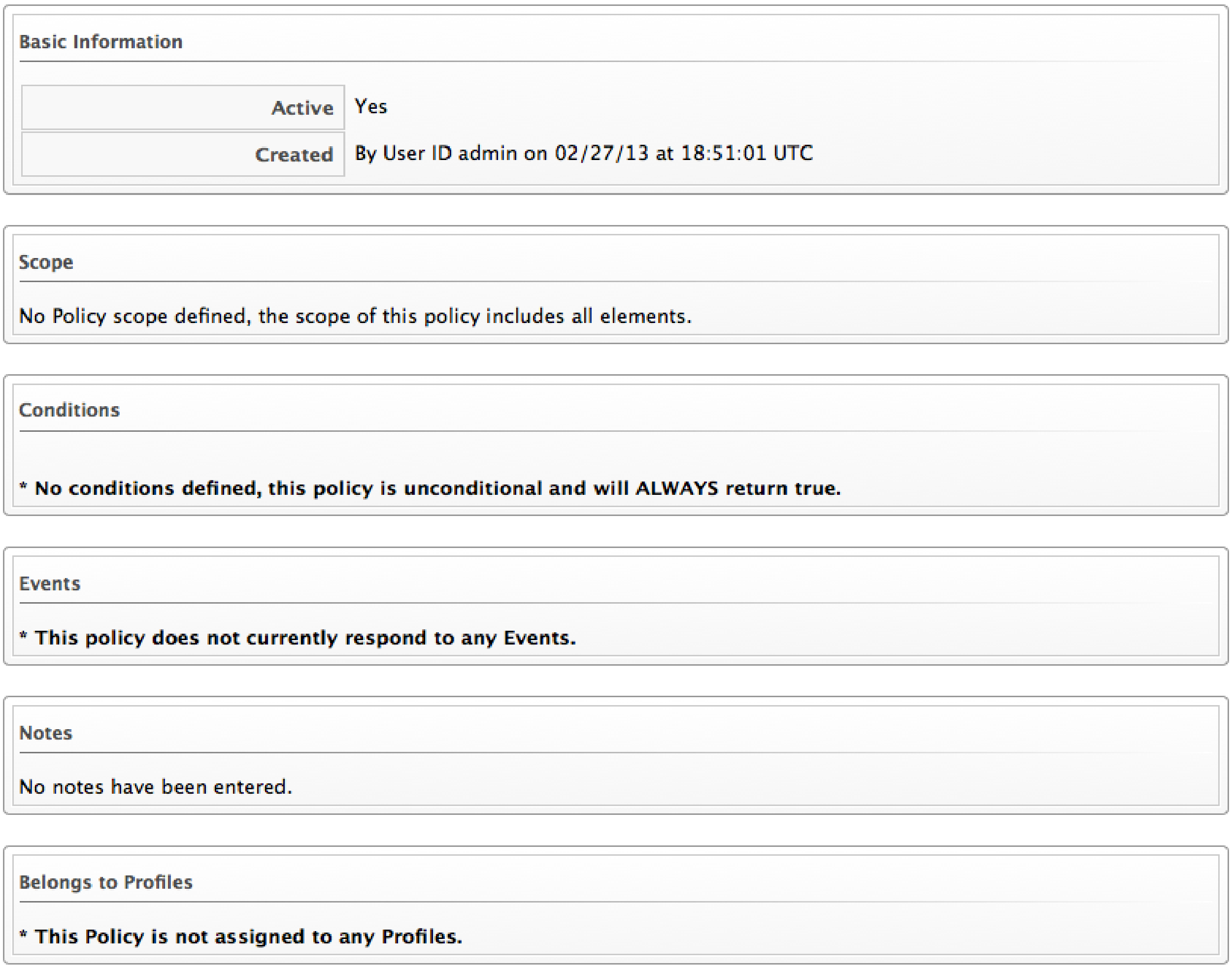
Active ☑

6. Uncheck **Active** if you do not want this policy processed even when assigned to a resource.

7. You can enter a **Scope** here (You can also create a scope as part of a condition, or not use one at all). If the host or virtual machine is not included in the scope, no actions will be run.

8. In the **Notes** area, add a detailed explanation of the policy.

9. Click **Add**. You are brought to the page where you add conditions and events to your new policy.



Basic Information

Active: Yes

Created: By User ID admin on 02/27/13 at 18:51:01 UTC

Scope

No Policy scope defined, the scope of this policy includes all elements.

Conditions

* No conditions defined, this policy is unconditional and will ALWAYS return true.

Events

* This policy does not currently respond to any Events.

Notes

No notes have been entered.

Belongs to Profiles

* This Policy is not assigned to any Profiles.

10. Click ⚙ (**Configuration**) to associate conditions, events, and actions with the policy.

2.1.2. Editing Basic Information, Scope, and Notes for a Policy

As your enterprise's needs change, you can change the name of a policy or its scope. If the items being evaluated are out of scope, policy processing stops and no actions run.

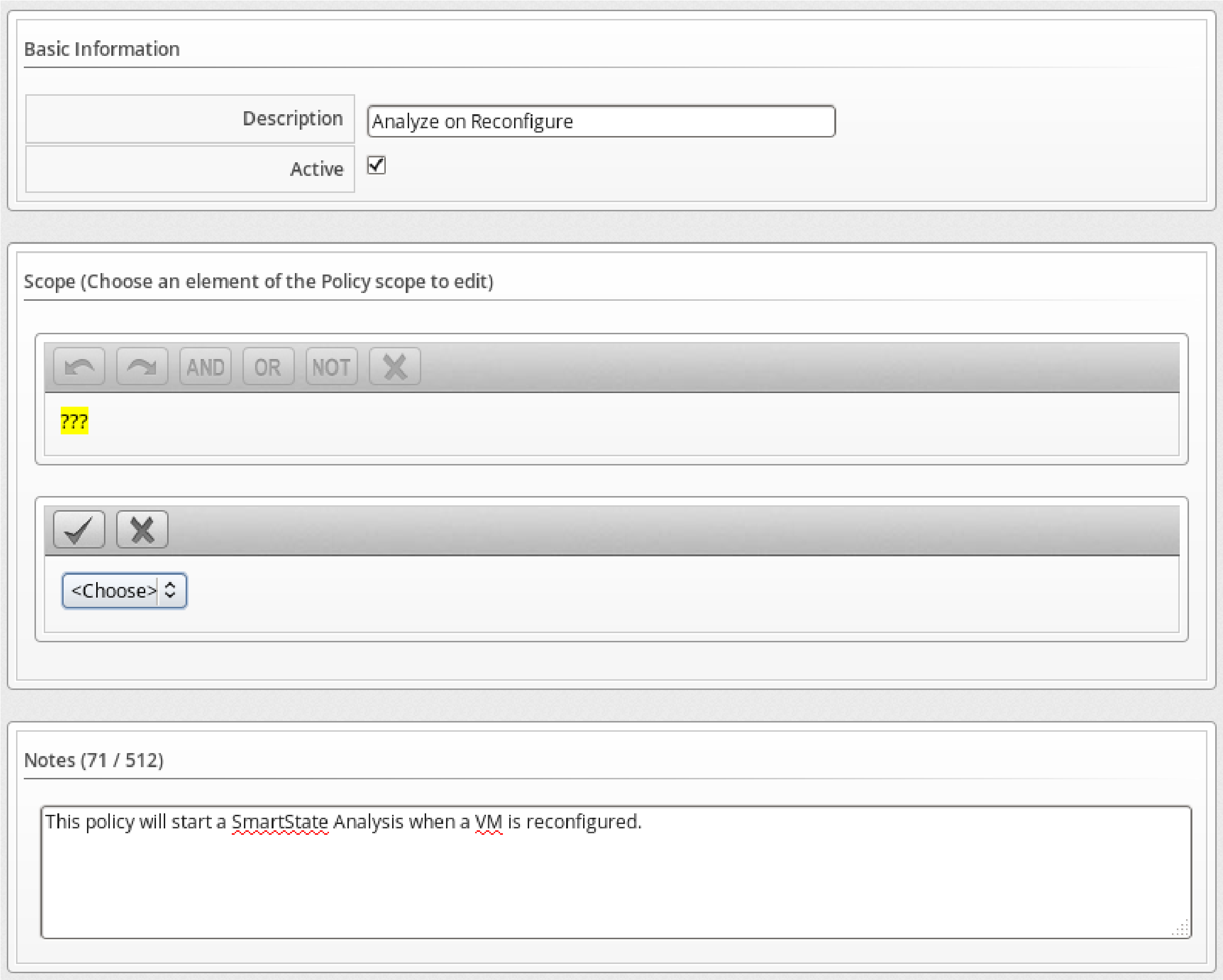
Procedure 2.2. To Edit Basic Information and Scope for a Policy

1. Navigate to **Control** → **Explorer**.

2. Click the **Policies** accordion, and select the policy to edit.

3. Click ⚙ (**Configuration**), ✏ (**Edit Basic Info, Scope, and Notes**).

4. In the **Scope** area, create a general condition based on a simple attribute. Or, click on an existing expression to edit it. Based on what you choose, different options appear. Recall that a scope is optional for a policy.



Basic Information

Description	Analyze on Reconfigure
Active	☑

Scope (Choose an element of the Policy scope to edit)

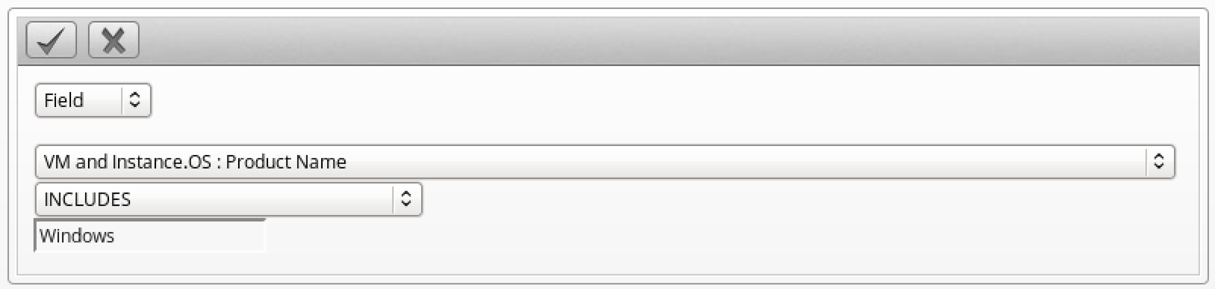
???

<Choose>

Notes (71 / 512)

This policy will start a SmartState Analysis when a VM is reconfigured.

- Click **Field** to create criteria based on field values.



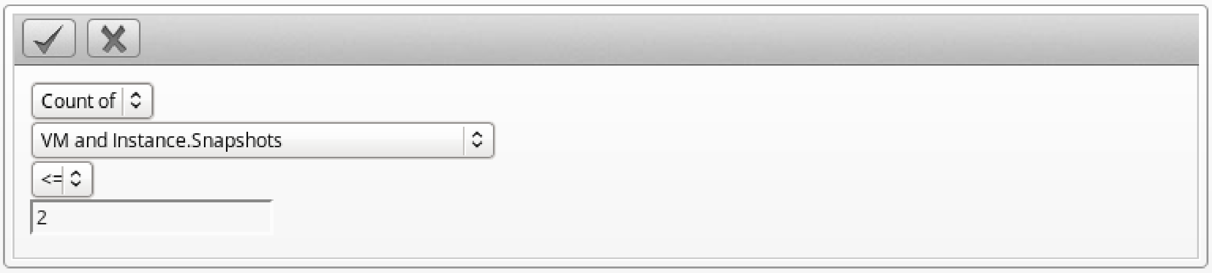
Field

VM and Instance.OS : Product Name

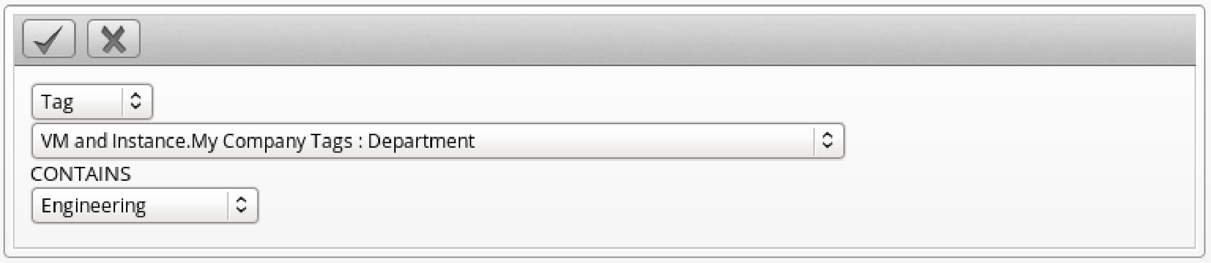
INCLUDES

Windows

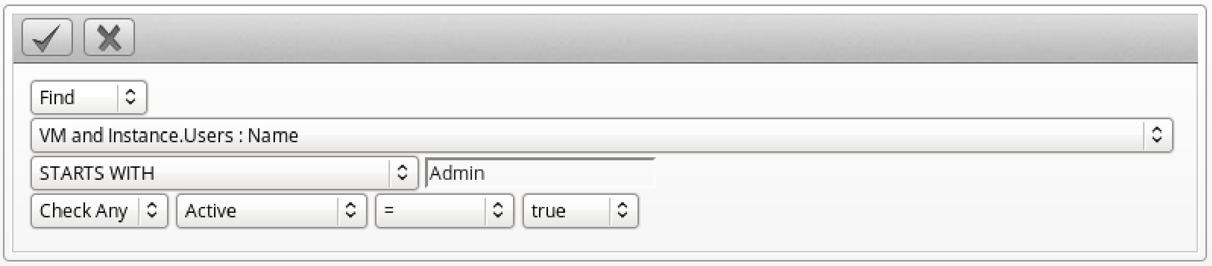
- Click **Count of** to create criteria based on the count of something, such as the number of snapshots for a virtual machine, or the number of virtual machines on a host.


Count of
VM and Instance.Snapshots
<=
2

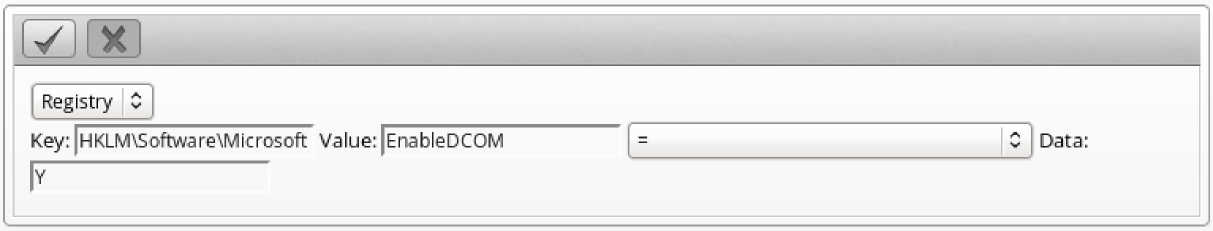
- Click **Tag** to create criteria based on tags assigned to your resources. For example, you can check the power state of a virtual machine or see if it is tagged as production.


Tag
VM and Instance.My Company Tags : Department
CONTAINS
Engineering

- Click **Find** to seek a particular value, and then check a property. For example, finding the **Admin** account and checking that it is enabled. Use the following check commands:
  - **Check Any**: The result is true if one or more of the find results satisfy the check condition.
  - **Check All**: All of the find results must match for a true result.
  - **Check Count**: If the result satisfies the expression in check count, the result is true.


Find
VM and Instance.Users : Name
STARTS WITH Admin
Check Any Active = true

- Click **Registry** to create criteria based on registry values. For example, you can check if DCOM is enabled on a Windows System. Note that this applies only to Windows operating systems. Registry will only be available if you are editing a VM Control Policy.


Registry
Key: HKLM\Software\Microsoft Value: EnableDCOM = Data:
Y

5. Click ✓ (**Commit Expression Element Changes**) to add the scope.

6. In the **Notes** area, make the required changes.

7. Click **Save**.

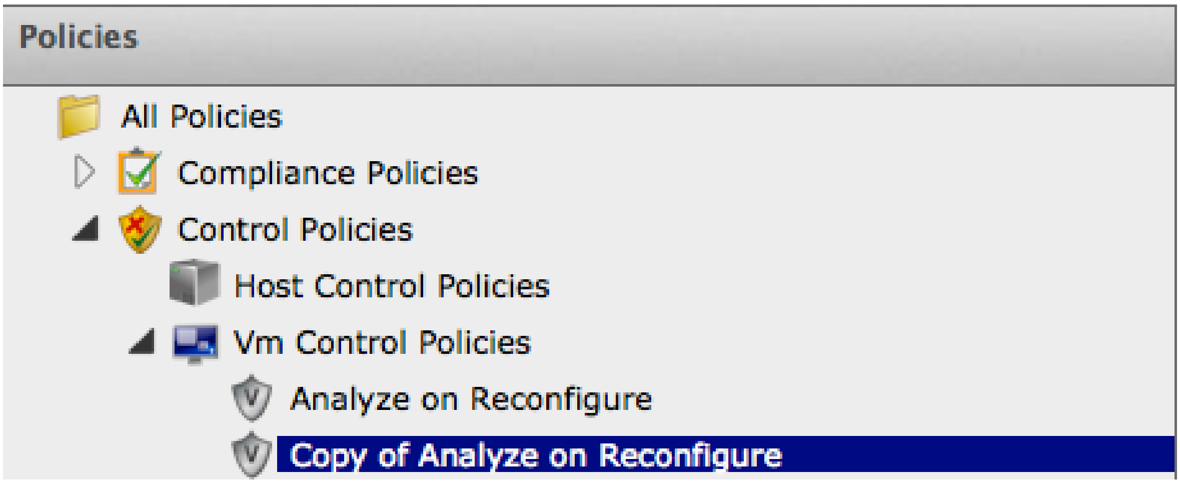
2.1.3. Copying a Policy

You can copy a policy if its contents are similar to a new one that you want to create, then change the condition or event associated with it. This enables you to make new policies efficiently.

Procedure 2.3. To Copy a Policy

1. Navigate to **Control** → **Explorer**.

2. Click the **Policies** accordion, and select the policy you want to copy.



3. Click (**`Configuration`**), (**`Copy this Policy to new Policy`**).

4. Click **`OK`** to confirm.

Result:

The new policy is created with a prefix of **`Copy of`** in its description, and it can be viewed in the **`Policy`** accordion.

2.1.4. Deleting a Policy

You can remove policies that you no longer need. You can only remove policies that are not assigned to a policy profile.

Procedure 2.4. To Delete a Policy

1. Navigate to **Control** → **Explorer**.

2. Click the **Policies** accordion, and select the policy you want to remove.

3. Click (**`Configuration`**), (**`Delete this Host/VM and Instance Policy`**).

4. Click **`OK`** to confirm.

2.1.5. Creating a New Policy Condition

If you have not already created a condition to use with this policy, you can create one directly from inside the policy. A condition can contain two elements, a scope, and an expression. The expression is mandatory, but the scope is optional. A scope is a general attribute that is quickly checked before evaluating a more complex expression. You can create a scope at either the policy or condition level.

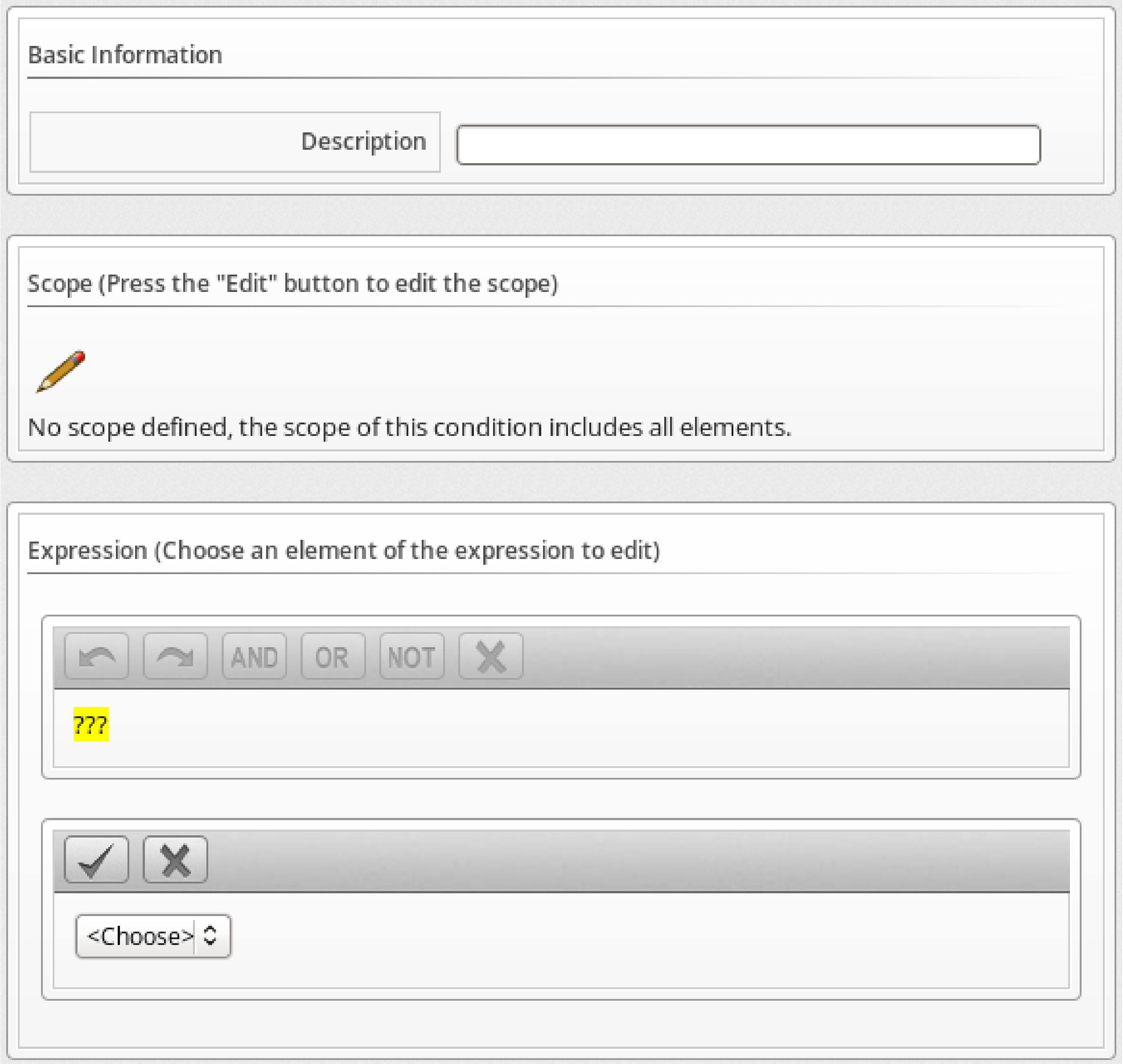
Procedure 2.5. To Create a New Condition Assigned to a Policy

1. Navigate to **Control** → **Explorer**.

2. Click the **Policies** accordion, and select the policy you want to create a new condition for.

3. Click ⚙ (**Configuration**), (**Create a new Condition assigned to this Policy**).

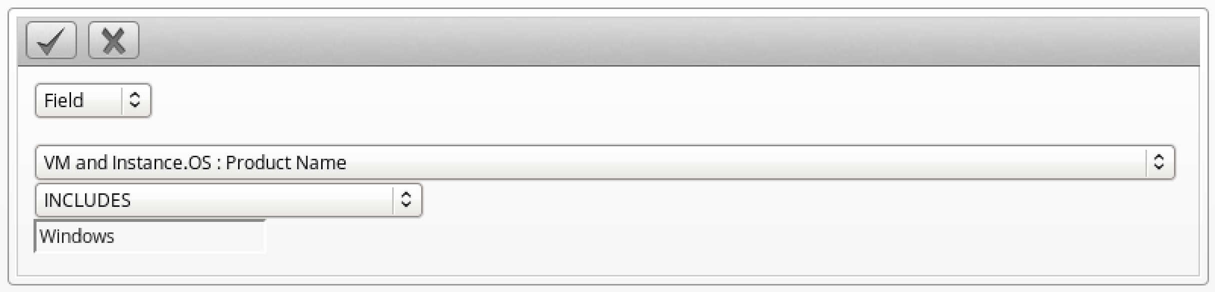
4. Type in a **Description** for the condition. It must be unique to all the conditions.



Basic Information
Description
Scope (Press the "Edit" button to edit the scope)
No scope defined, the scope of this condition includes all elements.
Expression (Choose an element of the expression to edit)
AND
OR
NOT
???
<Choose>

5. Click (**Edit this Scope**) in the **Scope** area to create a general expression based on a simple attribute, such as operating system version. Based on what you choose, different options display. Scope is optional.

   - Click **Field** to create criteria based on field values.



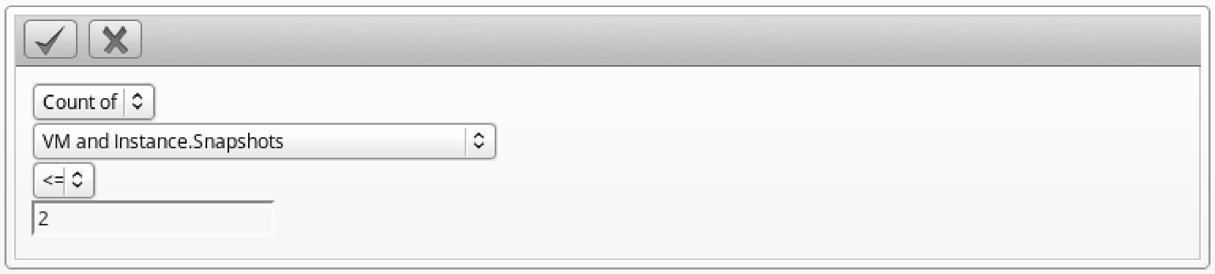
Field

VM and Instance.OS : Product Name

INCLUDES

Windows

- Click **Count of** to create criteria based on the count of something, such as the number of snapshots for a virtual machine, or the number of virtual machines on a host.



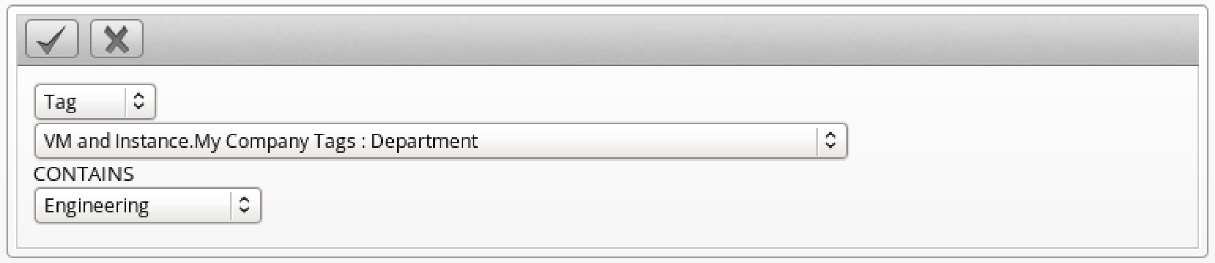
Count of

VM and Instance.Snapshots

<=

2

- Click **Tag** to create criteria based on tags assigned to your resources. For example, you can check the power state of a virtual machine or see if it is tagged as production.



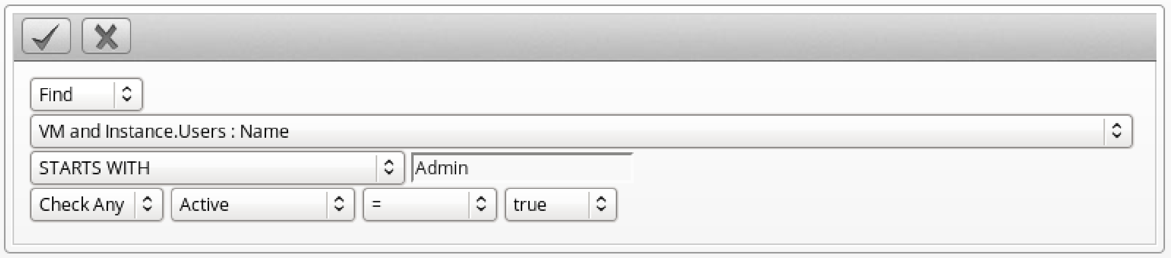
Tag

VM and Instance.My Company Tags : Department

CONTAINS

Engineering

- Click **Find** to seek a particular value, and then check a property. For example, finding the Admin account and checking that it is enabled. Use the following check commands:
  - **Check Any**: The result is true if one or more of the find results satisfy the check condition.
  - **Check All**: All of the find results must match for a true result.
  - **Check Count**: If the result satisfies the expression in check count, the result is true.



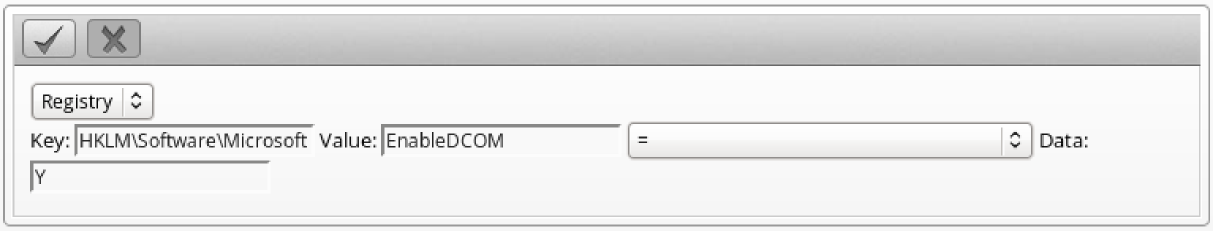
Find

VM and Instance.Users : Name

STARTS WITH Admin

Check Any Active = true

- Click **Registry** to create criteria based on registry values. For example, you can check if DCOM is enabled on a Windows System. Note that this applies only to Windows operating systems. Registry is only available if you are creating a VM Control Policy.



Registry

Key: HKLM\Software\Microsoft Value: EnableDCOM = Data: Y

6. Click ✓ (**Commit expression element changes**) to add the scope.

7. Click ✎ (**Edit this Expression**) in the **Expression** area. Based on what you choose, options display as per the choices presented in the **Scope** area detailed above.

8. Click ✓ (**Commit Expression Element Changes**) to add the expression.

9. In **Notes**, type in a detailed explanation of the condition.

10. Click **Add**.

Result:

The condition is created and is assigned directly to the policy. Note that the condition can be assigned to other policies.

2.1.6. Editing Policy Condition Assignments

Use this procedure to use a condition that has already been created either separately or as part of another policy. You can also remove a condition from a policy that no longer applies.

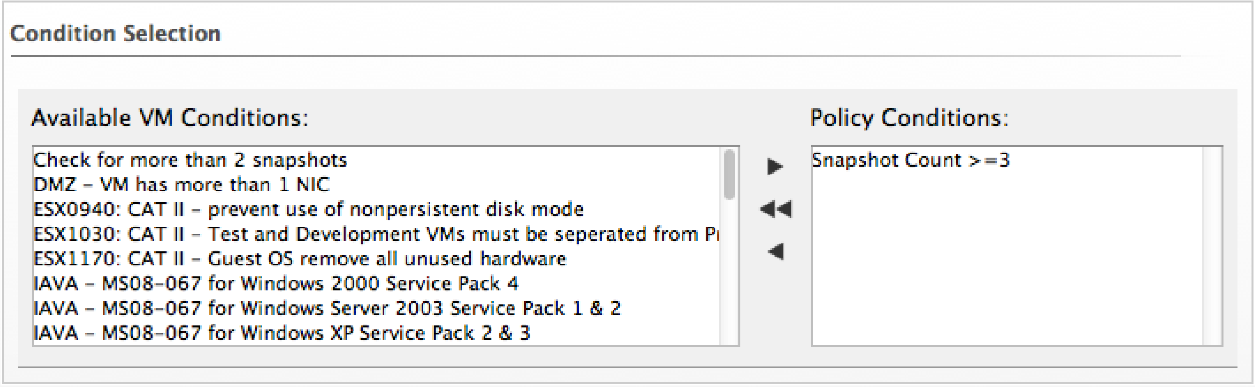
Procedure 2.6. To Edit Policy Condition Assignments

1. Navigate to **Control** → **Explorer**.

2. Click the **Policies** accordion, and select the policy you want to assign conditions to.

3. Click ⚙ (**Configuration**), ◆ (**Edit this Policy's Condition assignments**).

4. From the **Condition Selection** area, you can assign conditions to the policy, remove all conditions from the policy, or remove specific conditions from the policy.



Condition Selection

Available VM Conditions:

Check for more than 2 snapshots
DMZ - VM has more than 1 NIC
ESX0940: CAT II - prevent use of nonpersistent disk mode
ESX1030: CAT II - Test and Development VMs must be seperated from Pı
ESX1170: CAT II - Guest OS remove all unused hardware
IAVA - MS08-067 for Windows 2000 Service Pack 4
IAVA - MS08-067 for Windows Server 2003 Service Pack 1 & 2
IAVA - MS08-067 for Windows XP Service Pack 2 & 3

Policy Conditions:

Snapshot Count >=3

   - To add one or some conditions, select all the conditions you want to apply from the **`Available Conditions`** box. Use **`Ctrl`** to add multiple conditions to a policy. Then, click ▶ (**`Move selected Conditions into this Policy`**).
   - Click ◀◀ (**`Remove all Conditions from this Policy`**) to unassign any conditions from this policy.
   - To remove one or some conditions, select all the conditions you want to remove from the **`Policy Conditions`** box. Use **`Ctrl`** to select multiple conditions. Then, click ◀ (**`Remove selected Conditions from this Policy`**)

5. Click **Save**.

2.1.7. Editing Policy Event Assignments

The policy evaluates its scopes and conditions when specified events occur in your virtual infrastructure. This procedure enables you to select those events and the actions that should occur based on the evaluation of the scopes and conditions for the policy.

Procedure 2.7. To Edit a Policy's Event Assignments

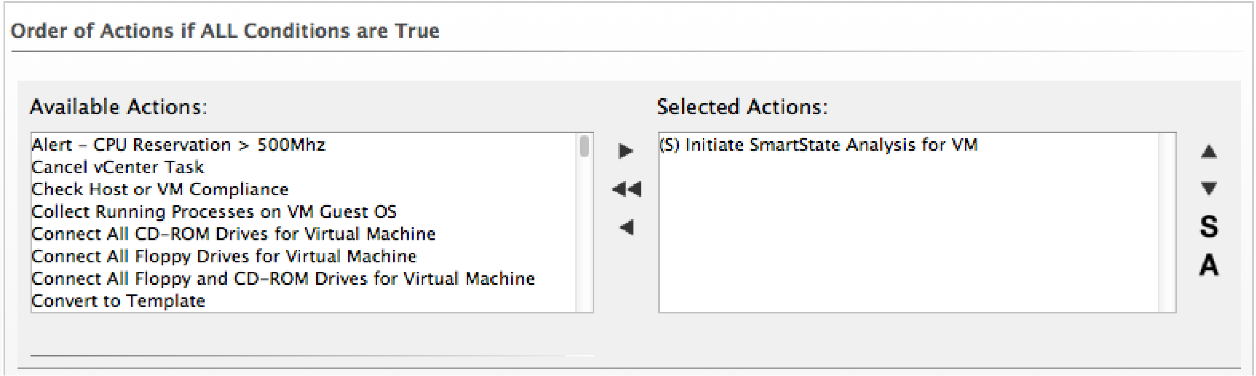
1. Navigate to **Control** → **Explorer**.
2. Click the **Policies** accordion and select the control policy you want to assign events to.
3. Click ⚙ (**`Configuration`**), (**`Edit this Policy's Event assignments`**).
4. Check all the events you want to assign to this policy. For a description of the events, see *Events*.
5. Click **Save**.

2.1.8. Assigning an Action to an Event

This procedure describes how to assign an action to an event.

Procedure 2.8. To Assign an Action to an Event

1. Navigate to **Control** → **Explorer**.
2. Click the **Policies** accordion, and select the policy you want to assign actions to.
3. From the **Events** area, click on the description of the event you want to assign an action to.
4. Click ⚙ (**`Configuration`**), (**`Edit Actions for this Policy Event`**).
5. Select all the appropriate actions from the **`Available Actions`** box, inside the **Order of Actions if ALL Conditions are True**. These are the actions that will take place if the resources meet the Condition of the Policy.



Order of Actions if ALL Conditions are True

Available Actions:

- Alert - CPU Reservation > 500Mhz
- Cancel vCenter Task
- Check Host or VM Compliance
- Collect Running Processes on VM Guest OS
- Connect All CD-ROM Drives for Virtual Machine
- Connect All Floppy Drives for Virtual Machine
- Connect All Floppy and CD-ROM Drives for Virtual Machine
- Convert to Template

Selected Actions:

- (S) Initiate SmartState Analysis for VM

> **Note**
>
> Each selected action can be executed synchronously or asynchronously; synchronous actions will not start until the previous synchronous action is completed, and asynchronous action allows the next action to start whether or not the first action has completed. Also, at least one CloudForms Management Engine server in the CloudForms Management Engine zone must have the notifier server role enabled for the trap to be sent.

6. Click the add button (▶), then:

   - Click the action, then click **A** (**Set selected Actions to Asynchronous**) to make it asynchronous.

   - Click the action, then click **S** (**Set selected Actions to Synchronous**) to make it synchronous. If creating a synchronous action, use the up and down arrows to identify in what order you want the actions to run.

7. Select all the actions from the appropriate **`Available Actions`** box, inside of the **Order of Actions if ANY Conditions are False**. These are the actions that take place if the resources do not meet the condition of the policy.

8. Click **Save**.

2.2. Compliance Policies

Compliance policies are specifically designed to secure your environment by checking conditions that you create. These conditions can include the same conditions that you would use in a control policy, and most of the procedures are the same. However, a compliance policy automatically assigns the mark as a compliant action when the virtual machine or host passes all of the conditions. If any of the conditions are not met, then the virtual machine or host is marked as non-compliant. The compliance status is shown in the summary screen for the virtual machine or host and on the compare and drift screens.

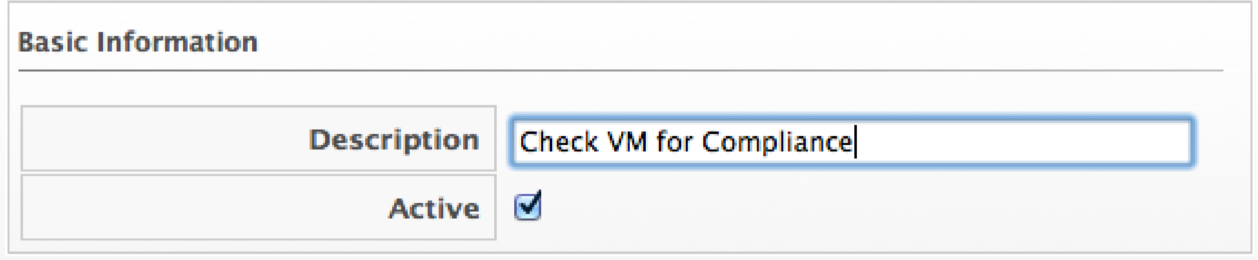
2.2.1. Creating a Compliance Policy

Create compliance policies by assigning or creating a condition. CloudForms Management Engine automatically assigns the events and actions to the compliance policy as opposed to a control policy where you must define this yourself. The VM or host compliance check event is assigned to the compliance policy. A compliance policy runs the mark as compliant action when the virtual machine or host passes all of the conditions. If any of the conditions are not met, then the virtual machine or host is marked as non-compliant.

If you do not know how to create a condition, see Section 2.1.5, “Creating a New Policy Condition”. Carefully plan the purpose of your policy before creating it. You can also use a scope expression that is tested immediately when the compliance check event triggers the policy. If the item is out of scope, then the policy does not continue on to the conditions, and none of the associated actions run.

Procedure 2.9. To Create a Compliance Policy

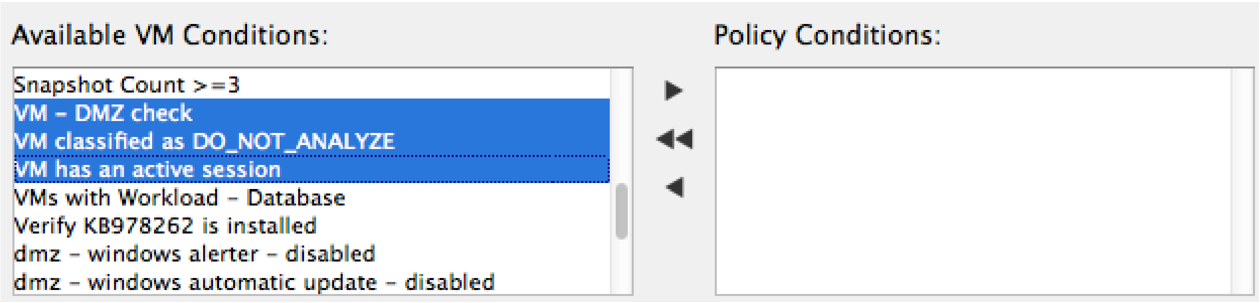
1. Navigate to **Control** → **Explorer**.
2. Click on the **Policies** accordion, and select VM or host compliances policies.
3. Click ⚙ (**Configuration**), ✚ (**Add a new Compliance Policy**).
4. Type in a **Description** for the policy.



Basic Information

Description	Check VM for Compliance
Active	☑

5. Uncheck **Active** if you do not want this policy processed even when assigned to a resource.
6. You can enter a scope here. (You can also create a scope as part of a condition, or not use one at all.) If the host or virtual machine is not included in the scope, NO actions run.
7. In the **Notes** area, add a detailed explanation of the policy.
8. Click **Add**.
9. Click ⚙ (**Configuration**), ◆ (**Edit this Policy's Condition assignments**).
10. Select the required conditions from the **Available Conditions** box. Use the **Ctrl** key to select multiple actions.



Available VM Conditions:

Snapshot Count >=3
VM - DMZ check
VM classified as DO_NOT_ANALYZE
VM has an active session
VMs with Workload - Database
Verify KB978262 is installed
dmz - windows alerter - disabled
dmz - windows automatic update - disabled

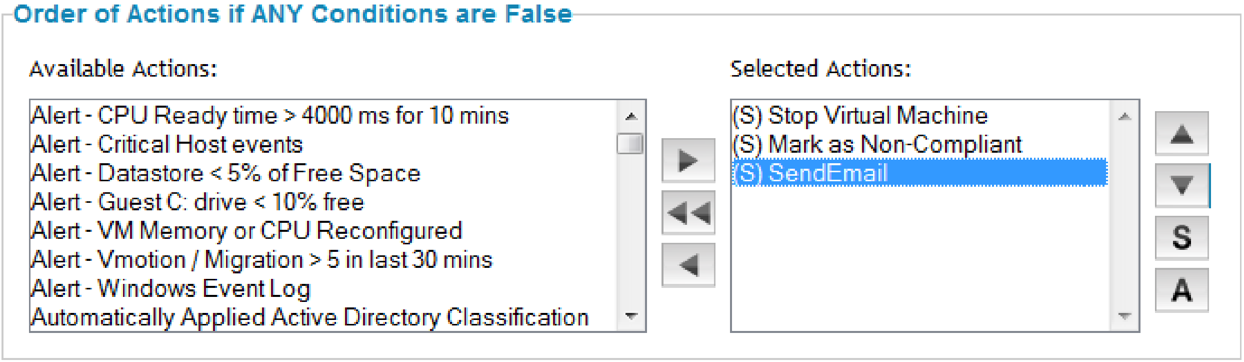
Policy Conditions:

11. Click ▶ (**Move selected Conditions into this Policy**).
12. Click **Save**. By default, if ANY of the conditions are false, the virtual machine is marked as non-compliant.

13. To add other actions, such as sending an email if the virtual machine fails the compliance test, click **VM Compliance Check**.

14. Click ⚙ (**Configuration**), ✎ (**Edit Actions for this Policy Event**).

15. Select **Stop Virtual Machine** and **Send Email** from the **Available Actions** area in **Order of Actions if ANY conditions are False**. (**Mark as Non-Compliant** should already be selected.)



Order of Actions if ANY Conditions are False

Available Actions:

- Alert - CPU Ready time > 4000 ms for 10 mins
- Alert - Critical Host events
- Alert - Datastore < 5% of Free Space
- Alert - Guest C: drive < 10% free
- Alert - VM Memory or CPU Reconfigured
- Alert - Vmotion / Migration > 5 in last 30 mins
- Alert - Windows Event Log
- Automatically Applied Active Directory Classification

Selected Actions:

- (S) Stop Virtual Machine
- (S) Mark as Non-Compliant
- (S) SendEmail

16. Click ▶ (**Move selected Actions into this Event**).

17. Click **Add**.

You can now make this part of a policy profile. After assigning the policy profile to the virtual machine, you can check it for its compliance status either on a schedule or on demand.

2.2.2. Creating a Compliance Condition to Check Host File Contents

CloudForms Management Engine Control provides the ability to create a compliance condition that checks file contents. Use this to be sure that internal operating system settings meet your security criteria. Regular expressions are used to create the search pattern. Test your regular expressions thoroughly before using them in a production environment.

Note that to search file contents you will need to have collected the file using a host analysis profile. See the *CloudForms Management Engine Insight Guide* for instructions.

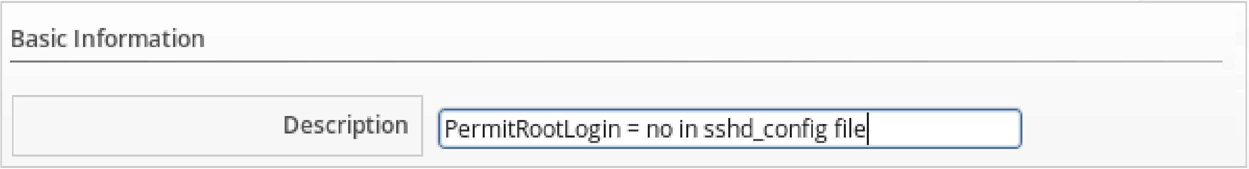
Procedure 2.10. To Create a Condition to Check Host File Contents

1. Navigate to **Control** → **Explorer**.

2. Click the **Conditions** accordion, and select **Host Conditions**.

3. Click ⚙ (**Configuration**), ✚ (**Add a New Host Condition**).

4. In **Basic Information**, type in a **Description** for the condition.



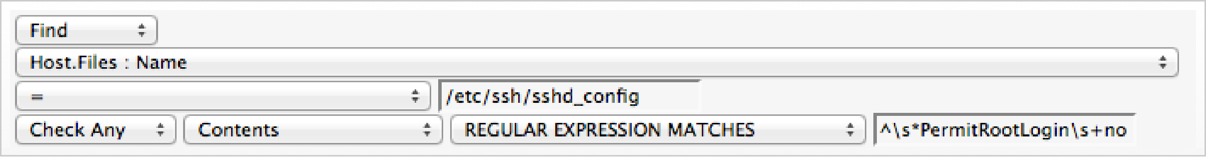
Basic Information

Description: PermitRootLogin = no in sshd_config file

5. Editing the **Scope** area is not necessary for this procedure. Skip editing any **Scope** conditions.

6. If the **Expression** area is not automatically opened, click ✎ (**Edit this Expression**), then edit the condition area to create a general condition based on a simple attribute. Based on what you choose, different options appear.

   - Click **Find**, then **Host.Files : Name**, and the parameters to select the file that you want to check.
   - Click **Check Any**, **Contents**, **Regular Expression Matches**, and type the expression. For example, if you want to make sure that permit root login is set to no, type **^\s*PermitRootLogin\s+no**.



Find
Host.Files : Name
= /etc/ssh/sshd_config
Check Any Contents REGULAR EXPRESSION MATCHES ^\s*PermitRootLogin\s+no

7. Click ✓ (**Commit expression element changes**) to add the expression.
8. In **Notes** area, type in a detailed explanation of the condition.
9. Click **Add**.

2.2.3. Checking for Compliance

After you have created your compliance policies and assigned them to a policy profile, you can check compliance in two ways. You can either schedule the compliance check or perform the check directly from the summary screen.

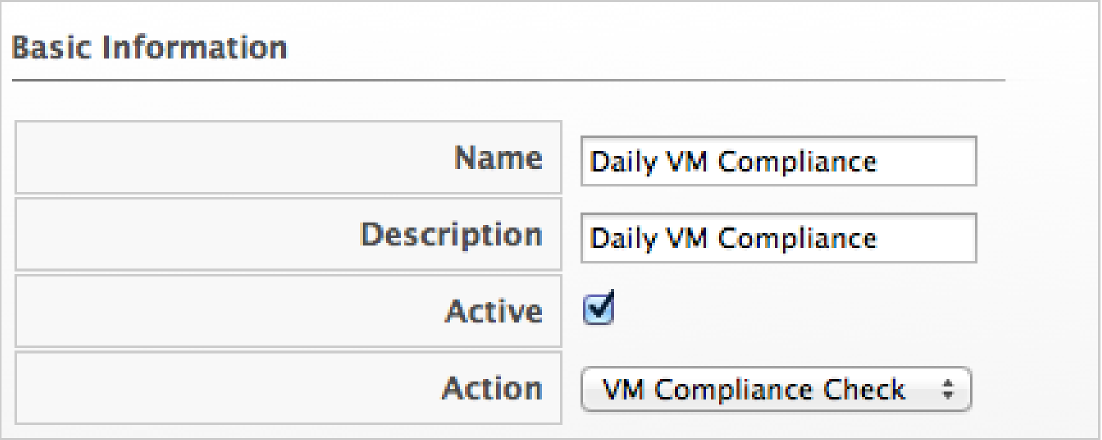
The compliance check runs all compliance policies that are assigned to the host or virtual machine. If the item fails any of the checks, it is marked as non-compliant in the item's summary screen.

> **Note**
>
> To schedule, you must have **EvmRole-administrator** access to the CloudForms Management Engine server.

2.2.3.1. Scheduling a Compliance Check

Procedure 2.11. To Schedule a Compliance Check

1. Navigate to **Configure → Configuration**
2. Click the **Settings** accordion, and select **Schedules**.
3. Click ⚙ (**Configuration**), + (**Add a new Schedule**).
4. In the **Basic Information** area, type in a name and description for the schedule.



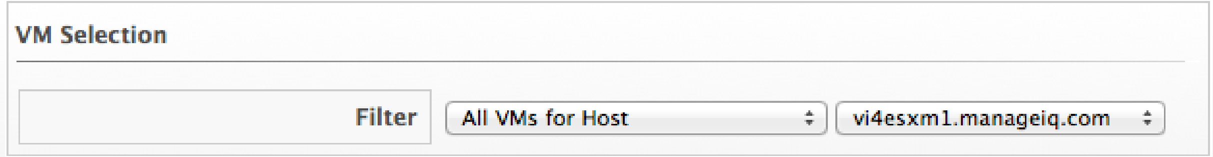
Basic Information

Name	Daily VM Compliance
Description	Daily VM Compliance
Active	☑
Action	VM Compliance Check

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

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

   - If you choose **VM Compliance Check**, you are presented with **VM Selection** where you can choose to check all VMs, all VMs for a specific provider, all VMs for a cluster, all VMs for a specific host, a single VM, or you can select VMs using a global filter.



VM Selection

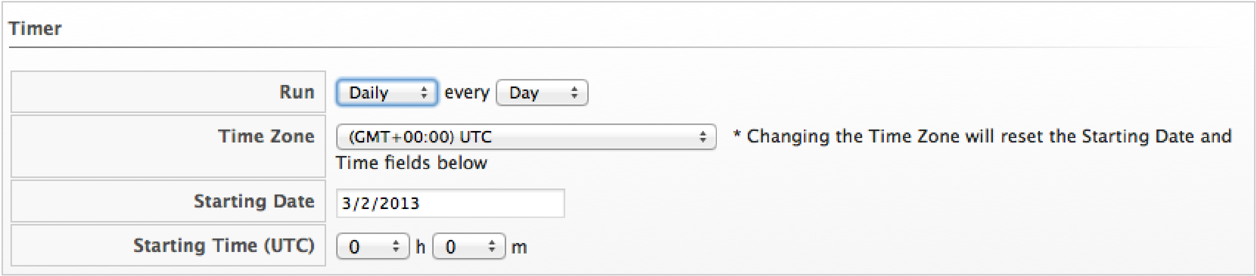
Filter	All VMs for Host	vi4esxm1.manageiq.com

   - If you choose **Host Compliance Check**, you are presented with **Host Selection** where you can choose to analyze all hosts, all hosts for a specific provider, all hosts for a cluster, a single host, or you can select hosts using a global filter.

Note

You can only schedule a host analysis 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.

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



Timer

Run	Daily every Day
Time Zone	(GMT+00:00) UTC * Changing the Time Zone will reset the Starting Date and Time fields below
Starting Date	3/2/2013
Starting Time (UTC)	0 h 0 m

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

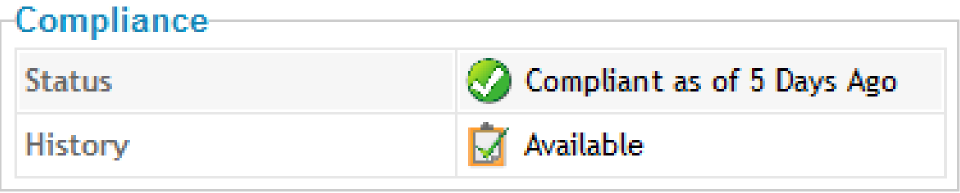
- Select **Daily** to run the analysis on a daily basis. You are prompted to select how many days you want between each analysis.
- Select **Hourly** to run the analysis hourly. You are prompted to select how many hours you want between each analysis.

8. Select the time zone for the schedule.
9. Type or select a date to begin the schedule in **Starting Date**.
10. Select a starting time based on a 24-hour clock in the selected time zone.
11. Click **Add**.

2.2.3.2. Checking a Virtual Machine for Compliance from the Summary Screen

Procedure 2.12. To Check a Virtual Machine for Compliance from the Summary Screen

1. Navigate to **Infrastructure** → **Virtual Machines**, click the virtual machine you want to check for compliance.
2. Click (**Policy**), and then (**Check Compliance of Last Known Configuration**).
3. A confirmation message appears. Click **OK**.
4. If it says **Available** next to **History** you can click it to view the compliance history.



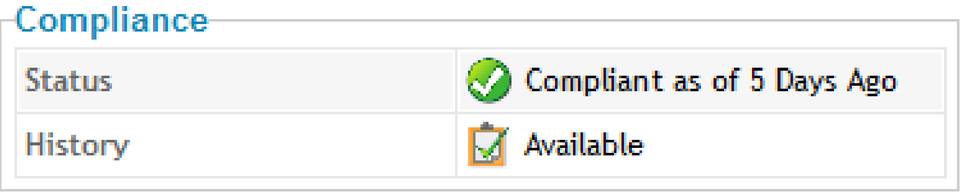
Compliance

Status	✓ Compliant as of 5 Days Ago
History	Available

2.2.3.3. Checking a Host for Compliance from the Summary Screen

Procedure 2.13. To Check a Host for Compliance from the Summary Screen

1. Navigate to **Infrastructure** → **Hosts**, click the host you want to check for compliance.
2. Click (**Policy**), and then (**Check Compliance of Last Known Configuration**) or (**Analyze then Check Compliance**).
3. To view the compliance history, click **Available** next to **History**.



Compliance

Status	✓ Compliant as of 5 Days Ago
History	Available

Chapter 3. Events

Events are triggers that cause a condition to be tested. CloudForms Management Engine Control provides several Events, that can be divided into functional types. Events cannot be modified.

Table 3.1. Event Types

Category	Description
Datastore Operation	Events related to datastore analysis.
Authentication Validation	Events related to credential validation for hosts and providers.
Company Tag	Events related to assigning and removing company tags from an infrastructure object.
Compliance	Events related to checking compliance policies.
Host Operation	Events related to the connection state of a host and status of a SmartState Analysis on a host.
VM Configuration	Events associated with a change in configuration of a virtual machine. These include, but are not limited to, clone, create, template create, and settings change.
VM Lifecycle	Events such as VM discovery, provisioning, and VM retirement.
VM Operation	Events associated with power states or locations of virtual machines and virtual desktop machines. These include, but are not limited to, power off, power on, reset, resume, VM shutdown, and suspend.

Each type has a set of events that you can select to trigger the checking of a condition.

Table 3.2. Events and Descriptions

Event	Description
Datastore Analysis Complete	Check the condition when a SmartState Analysis of datastore completes.
Datastore Analysis Request	Check the condition when a SmartState Analysis for a datastore is requested from the CloudForms Management Engine console.
Host Added to Cluster	Check the condition when a host is added to a cluster.
Host Analysis Complete	Check the condition when a SmartState Analysis of host completes.
Host Analysis Request	Check the condition when a SmartState Analysis is requested from the CloudForms Management Engine console.
Host Auth Changed	Check the condition when host authentication credentials are changed in the CloudForms Management Engine console.
Host Auth Error	Check the condition if there is any other error connecting to the host such as ssh/vim handshaking problems, timeouts, or any other uncategorized error.

Event	Description
Host Auth Incomplete Credentials	Check the condition if host authentication credentials are not complete in the CloudForms Management Engine console.
Host Auth Invalid	Check the condition if CloudForms Management Engine is able to communicate with the host and the credentials fail.
Host Auth Unreachable	Check the condition if CloudForms Management Engine is unable to communicate with the host.
Host Auth Valid	Check the condition when the host authentication credentials entered in the CloudForms Management Engine console are valid.
Host C & U Processing Complete	Check the condition when the processing of capacity and utilization data has finished.
Host Compliance Check	Check the condition when a compliance check is performed on a host.
Host Compliance Failed	Check the condition when a host fails a compliance check.
Host Compliance Passed	Check the condition when a host passes a compliance check.
Host Connect	Check the condition when a host connects to a provider.
Host Disconnect	Check the condition when a host disconnects from a provider.
Host Removed from Cluster	Check the condition when a host is removed from a cluster.
Provider Auth Changed	*For use only with CloudForms Management Engine automate, for future use in policies.* Check the condition when provider authentication credentials are changed in the CloudForms Management Engine console.
Provider Auth Error	*For use only with CloudForms Management Engine automate, for future use in policies.* Check the condition if there is any other error connecting to the provider such as ssh/vim handshaking problems, timeouts, or any other uncategorized error.
Provider Auth Incomplete Credentials	*For use only with CloudForms Management Engine automate, for future use in policies.* Check the condition if provider authentication credentials are not complete in the CloudForms Management Engine console.
Provider Auth Invalid	*For use only with CloudForms Management Engine automate, for future use in policies.* Check the condition if CloudForms Management Engine is able to communicate with the provider and the credentials fail.
Provider Auth Unreachable	*For use only with CloudForms Management Engine automate, for future use in policies.* Check the condition if CloudForms Management Engine is unable to communicate with the provider.

Event	Description
Provider Auth Valid	*For use only with CloudForms Management Engine automate, for future use in policies.* Check the condition when the provider authentication credentials entered in the CloudForms Management Engine console are valid.
Service Provision Complete	Check the condition when the service provision is complete.
Service Retired	Check the condition when the service has been retired.
Service Retirement Warning	Check the condition when the service is about to retire.
Service Start Request	Check the condition when the service has been requested to start.
Service Started	Check the condition when the service has started.
Service Stop Request	Check the condition when the service has been requested to stop.
Service Stopped	Check the condition when the service has stopped.
Tag Complete	Check the condition after a company tag is assigned.
Tag Parent Cluster Complete	Check the condition after a company tag is assigned to the virtual machines parent cluster.
Tag Parent Datastore Complete	Check the condition after a company tag is assigned to the virtual machines parent datastore.
Tag Parent Host Complete	Check the condition after a company tag is assigned to the virtual machines parent host.
Tag Parent Resource Pool Complete	Check the condition after a company tag is assigned to the virtual machines parent resource pool.
Tag Request	Check the condition when assignment of a company tag is attempted.
Un-Tag Complete	Check the condition when a company tag is removed.
Un-Tag Parent Cluster Complete	Check the condition after a company tag is removed from the virtual machines parent cluster.
Un-Tag Parent Datastore Complete	Check the condition after a company tag is removed from the virtual machines parent datastore.
Un-Tag Parent Host Complete	Check the condition after a company tag is removed from the virtual machines parent host.
Un-Tag Parent Resource Pool Complete	Check the condition after a company tag is assigned to the virtual machines parent resource pool.
Un-Tag Request	Check the condition when an attempt is made to remove a company tag.
VDI Connecting to Session	Check the condition when a VDI session is started.
VDI Disconnected from Session	Check the condition when a VDI session is disconnected.

Event	Description
VDI Login Session	Check the condition when a user logs on to a VDI session.
VDI Logoff Session	Check the condition when a user logs off from a VDI session.
VM Analysis Complete	Check the condition when a SmartState Analysis of virtual machine completes.
VM Analysis Failure	Check the condition when a SmartState Analysis of virtual machine fails.
VM Analysis Request	Check the condition when a SmartState Analysis is requested from the CloudForms Management Engine console.
VM Analysis Start	Check the condition when a SmartState Analysis of virtual machine is started.
VM C & U Processing Complete	Check the condition when the processing of capacity and utilization data has finished.
VM Clone Complete	Check the condition when a virtual machine is cloned.
VM Clone Start	Check the condition when a virtual machine clone is started.
VM Compliance Check	Check the condition when a compliance check is performed on a host.
VM Compliance Failed	Check the condition when a host fails a compliance check.
VM Compliance Passed	Check the condition when a host passes a compliance check.
VM Create Complete	Check the condition when a virtual machine is created.
VM Delete (from Disk) Request	Check the condition when someone tries to delete a virtual machine from disk from the CloudForms Management Engine console.
VM Discovery	Check the condition when CloudForms Management Engine discovers a virtual machine.
VM Guest Reboot	Check the condition when the virtual machine is rebooted.
VM Guest Reboot Request	Check the condition when someone tries to reboot a virtual machine from the CloudForms Management Engine console.
VM Guest Shutdown	Check the condition when the operating system of a virtual machine shuts down.
VM Guest Shutdown Request	Check the condition when someone tries to shutdown the operating system of a virtual machine from the CloudForms Management Engine console.
VM Live Migration (VMOTION)	Check the condition when a VMOTION is performed.
VM Power Off	Check the condition when a virtual machine is turned off.
VM Power Off Request	Check the condition when someone tries to power off a virtual machine from the CloudForms Management Engine console.

Event	Description
VM Power On	Check the condition when a virtual machine is turned on.
VM Power On Request	Check the condition when someone tries to turn on a virtual machine from the CloudForms Management Engine console.
VM Provision Complete	Check the condition when a VM is provisioned.
VM Remote Console Connected	Check the condition when the VM is connected to a remote console.
VM Removal from Inventory	Check the condition when a virtual machine is unregistered.
VM Removal from Inventory Request	Check the condition when a request is sent from the CloudForms Management Engine console to unregister a virtual machine.
VM Reset	Check the condition when a virtual machine is restarted.
VM Reset Request	Check the condition when a virtual machine is restarted from the CloudForms Management Engine console.
VM Retired	Check the condition when a virtual machine is retired.
VM Retirement Warning	Check the condition when a warning threshold is reached for retirement.
VM Settings Change	Check the condition when the settings of virtual machine are changed.
VM Snapshot Create Complete	Check the condition when a snapshot is completed.
VM Snapshot Create Request	Check the condition when someone tries to create a snapshot of a virtual machine from the CloudForms Management Engine console.
VM Snapshot Create Started	Check the condition when a snapshot creation is started.
VM Standby of Guest	Check the condition when the operating system of a virtual machine goes to standby.
VM Standby of Guest Request	Check the condition when someone tries to put the operating system of a virtual machine in standby from the CloudForms Management Engine console.
VM Suspend	Check the condition when a virtual machine is suspended.
VM Suspend Request	Check the condition when someone tries to suspend a virtual machine from the CloudForms Management Engine console.
VM Template Create Complete	Check the condition when a virtual machine template is created.

Chapter 4. Conditions

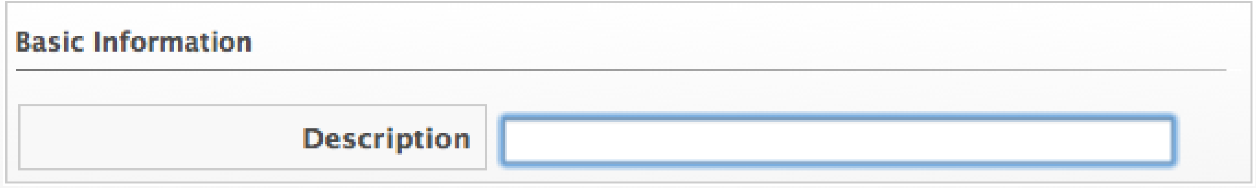
Conditions are tests performed on attributes of virtual machines. A condition can contain two elements, a scope, and an expression. The expression is mandatory, but the scope is optional. A scope is a general attribute that is quickly checked before evaluating a more complex expression. For example, you might use a scope to check the operating system, and use an expression to check for a specific set of applications or security patches that only apply to the operating system referenced in the scope. If no conditions, scope or expression, are defined for a policy, the policy is considered unconditional and returns a true value.

4.1. Creating a Condition

You can create a condition either from within a policy screen or by going directly to the expression editor in the CloudForms Management Engine console. You need to define a description and an expression element. The expression element defines what criteria you want to use to test the condition.

Procedure 4.1. To Create a Condition

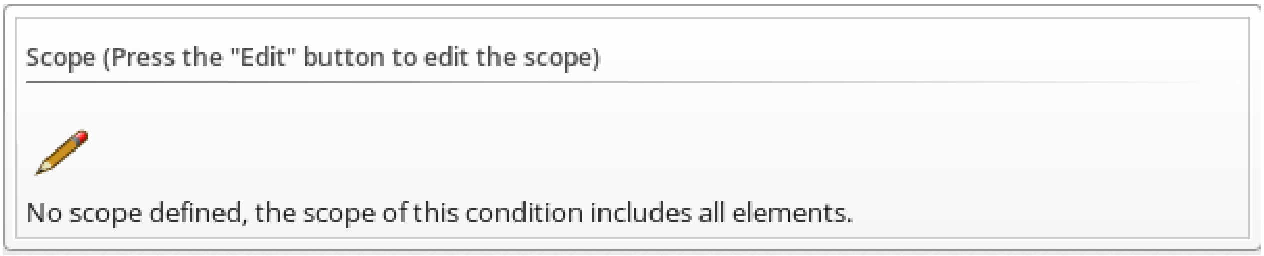
1. Navigate to **Control** → **Explorer**.
2. Click the **Conditions** accordion, and select either **Host Conditions** or **VM Conditions**.
3. Click ⚙ (**`Configuration`**), ✚ (**`Add a New Host`**).
4. Type in a **`Description`** for the condition.



Basic Information

Description

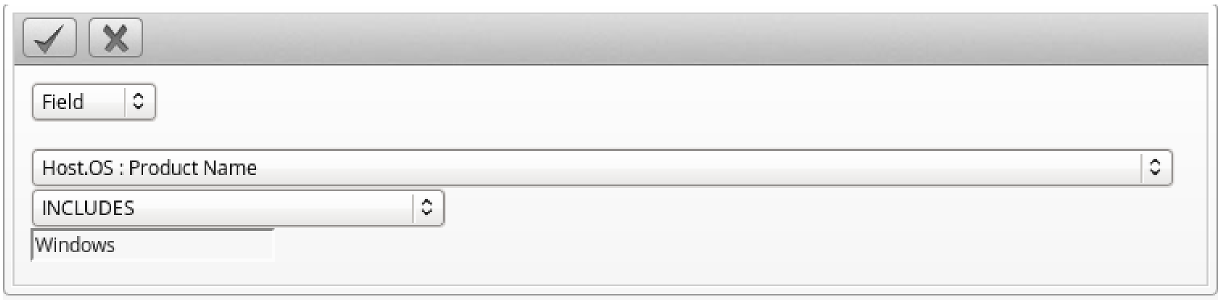
5. Click ✎ (**`Edit this Scope`**) in the **`Scope`** area to create a general condition based on a simple attribute. Based on what you choose, different options appear. Creating a scope is optional.



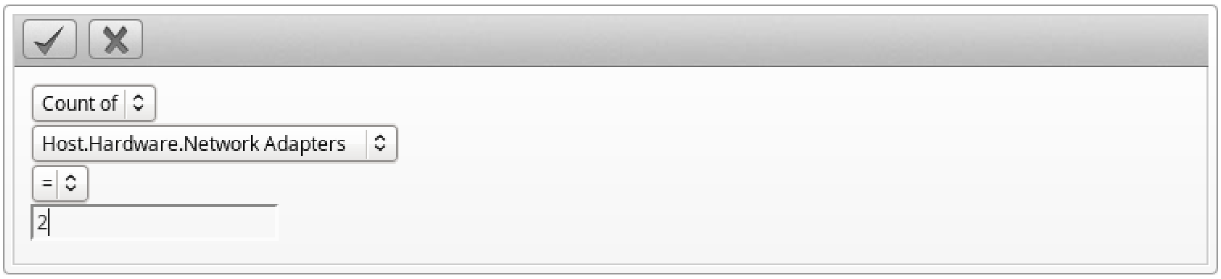
Scope (Press the "Edit" button to edit the scope)

No scope defined, the scope of this condition includes all elements.

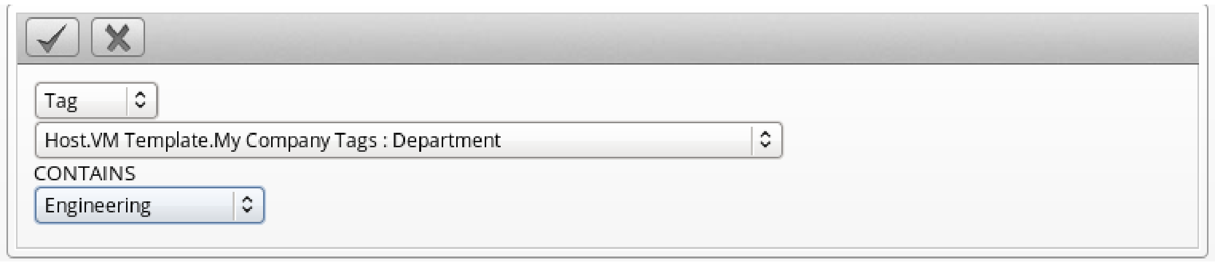
- Click **`Field`** to create criteria based on field values.


Field
Host.OS : Product Name
INCLUDES
Windows

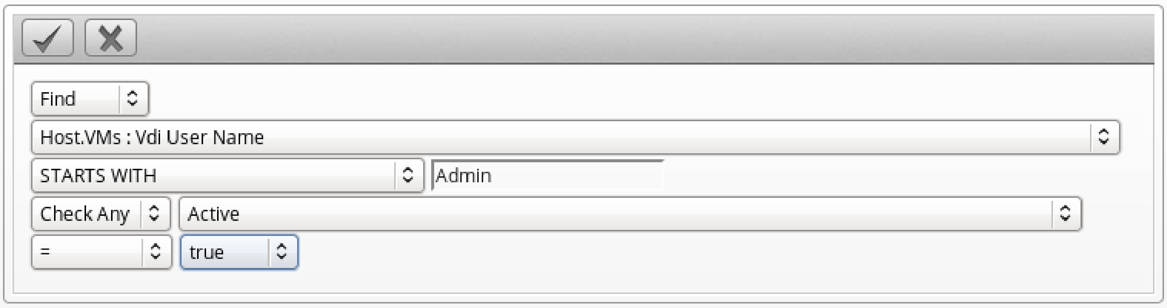
- Click **Count of** to create criteria based on the count of something, such as the number of network adapters on the host.


Count of
Host.Hardware.Network Adapters
=
2

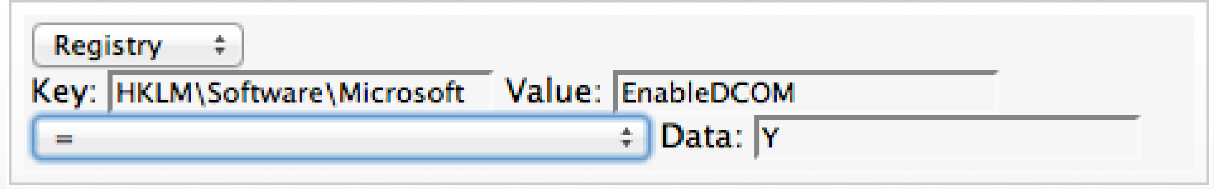
- Click **Tag** to create criteria based on tags assigned to your resources. For example, you can check the power state of a virtual machine or see if it is tagged as production.


Tag
Host.VM Template.My Company Tags : Department
CONTAINS
Engineering

- Click **Find** to seek a particular value, and then check a property. For example, finding the Admin account and checking that it is enabled. Use the following check commands:
  - **Check Any**: The result is true if one or more of the find results satisfy the check condition.
  - **Check All**: All of the find results must match for a true result.
  - **Check Count**: If the result satisfies the expression in check count, the result is true.


Find
Host.VMs : Vdi User Name
STARTS WITH
Admin
Check Any
Active
=
true

- Click **Registry** to create criteria based on registry values. For example, you can check if DCOM is enabled on a Windows System. Note that this applies only to Windows operating systems. Registry will only be available if you are creating a VM Condition.



Registry

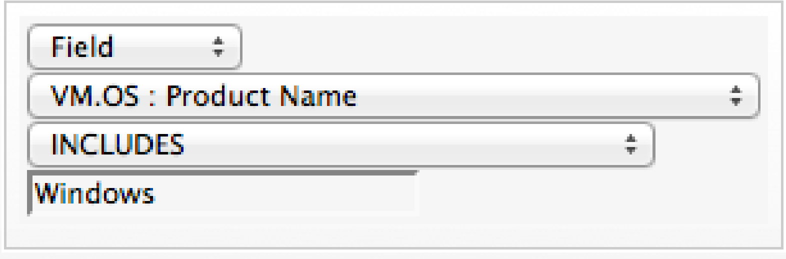
Key: HKLM\Software\Microsoft Value: EnableDCOM

= Data: Y

6. Click ✓ (**Commit Expression Element Changes**) to add the scope.

7. Click ✏ (**Edit this Condition**) in the **Expression** area to create a general condition based on a simple attribute. Based on what you choose, different options appear.

   - Click **Field** to create criteria based on field values.



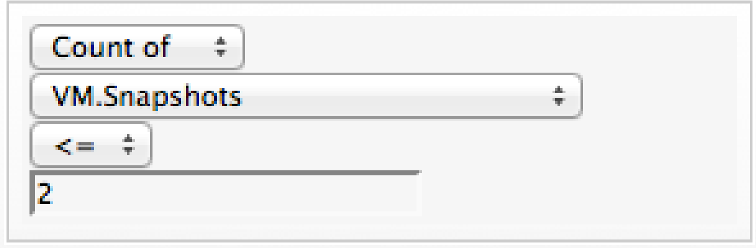
Field

VM.OS : Product Name

INCLUDES

Windows

   - Click **Count of** to create criteria based on the count of something, such as the number of snapshots for a virtual machine, or the number of virtual machines on a host.



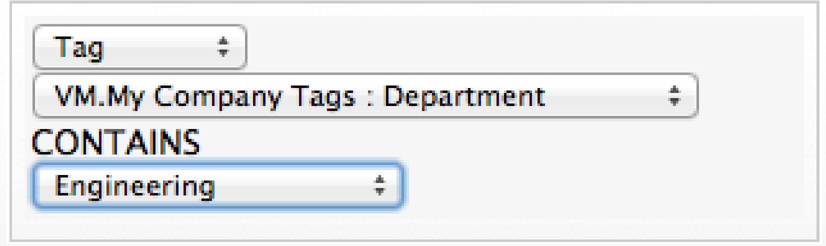
Count of

VM.Snapshots

<=

2

   - Click **Tag** to create criteria based on tags assigned to your resources. For example, you can check the power state of a virtual machine or see if it is tagged as production.



Tag

VM.My Company Tags : Department

CONTAINS

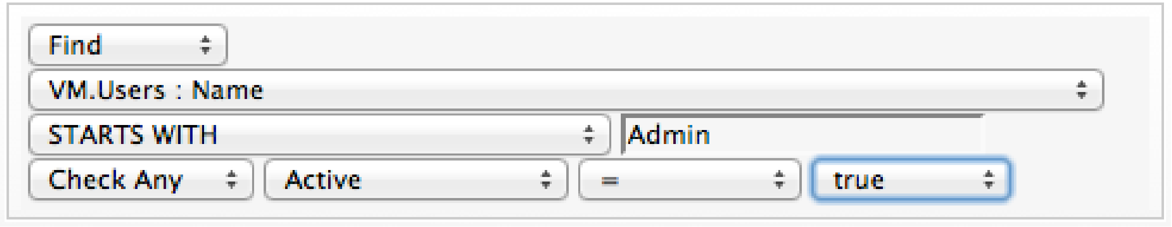
Engineering

   - Click **Find** to seek a particular value, and then check a property. For example, finding the Admin account and checking that it is enabled. Use the following check commands.

     - **Check Any**: The result is true if one or more of the find results satisfy the check condition.

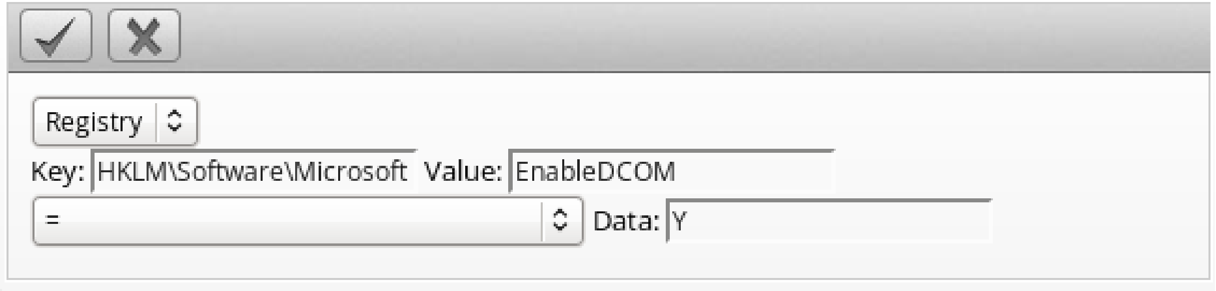
     - **Check All**: All of the find results must match for a true result.

     - **Check Count**: If the result satisfies the expression in check count, the result is true.



Find
VM.Users : Name
STARTS WITH Admin
Check Any Active = true

- Click **Registry** to create criteria based on registry values. For example, you can check if DCOM is enabled on a Windows System. Note that this applies only to Windows operating systems.



Registry
Key: HKLM\Software\Microsoft Value: EnableDCOM
= Data: Y

8. Click ✓ (**Commit Expression Element Changes**) to add the expression.

9. In **Notes**, type in a detailed explanation of the condition.

10. Click **Add**.

4.2. Editing a Condition

Edit a condition to add more expressions to it or modify its properties. You can edit conditions that you have created.

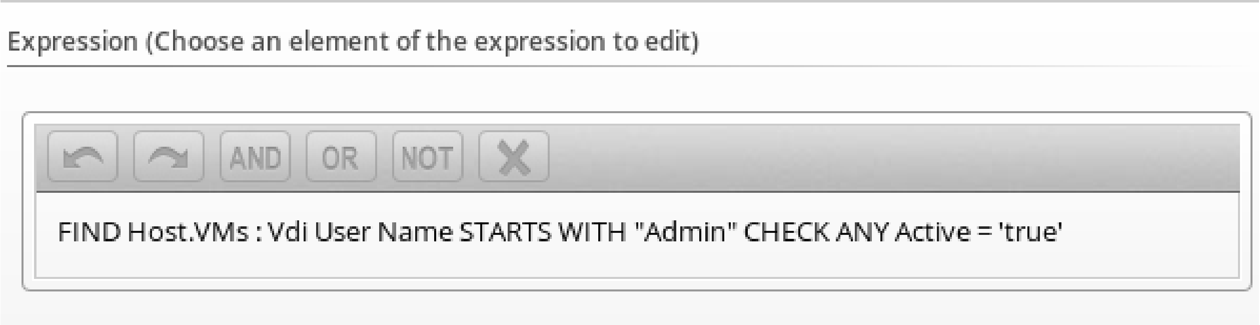
Procedure 4.2. To Edit a Condition

1. Navigate to **Control** → **Explorer**.

2. Click the **Conditions** accordion, and click on the condition you want to edit.

3. Click ⚙ (**Configuration**), ✎ (**Edit this Condition**).

4. Click in either the **Scope** or **Expression** area, and click the part of the condition to edit.



FIND Host.VMs : Vdi User Name STARTS WITH "Admin" CHECK ANY Active = 'true'

5. Make any edits for the current expression.

   - Click ✓ (**Commit expression element changes**) to add the changes.

- Click ↶ (**Undo the previous change**) to remove the change you just made.
- Click ↷ (**Redo the previous change**) to put the change that you just made back.
- Click AND (**AND with a new expression element**) to create a logical AND with a new expression element.
- Click OR (**OR with a new expression element**) to create a logical OR with a new expression element.
- Click NOT (**Wrap this expression element with a NOT**) to create a logical NOT on an expression element
- Click ✖ (**Remove this expression element**) to take out the current expression element.

6. When you have made all of the changes to the condition, click **Save**.

4.3. Copying a Condition

You can copy a condition to create a similar condition, then change the values associated with it. You can copy the sample conditions provided to customize them to your environment.

Procedure 4.3. To Copy a Condition

1. Navigate to **Control** → **Explorer**.
2. Click the **Conditions** accordion, and select the condition you want to copy.
3. Click ⚙ (**Configuration**), 🗐 (**Copy this Condition to a new Condition**).
4. Make any changes you need for the new condition. The description must be unique to all conditions.
5. Click **Add**.

4.4. Deleting a Condition

Remove conditions that are no longer applicable. You can only delete conditions that are not part of a policy. To be able to delete the condition, you must remove the policy first.

Procedure 4.4. To Delete a Condition

1. Navigate to **Control** → **Explorer**.
2. Click the **Conditions** accordion, and click on the condition you want to remove.
3. Click ⚙ (**Configuration**), 🗑 (**Delete this VM and Instance Condition**).

4. Click **OK** to confirm.

Chapter 5. Actions

Actions are performed after the condition is evaluated. CloudForms Management Engine Control comes with a set of default actions that you can choose from. You can also create some of your own.

Table 5.1. Default Actions and Descriptions

Action	Description
Cancel vCenter Task	Stop current vCenter Task. Due to limitations of vCenter, this applies only to cloning tasks.
Check Host or VM Compliance	Run compliance checks.
Collect Running Processes on VM Guest OS	Collect the list of running processes from the guest operating system.
Connect All CD-ROM Drives for Virtual Machine	Connect all the CD-ROM drives for the virtual Machine.
Connect All Floppy Drives for Virtual Machine	Connect all the floppy drives for the virtual machine.
Connect All Floppy and CD-ROM Drives for Virtual Machine	Connect all of the floppy and CD-ROM drives for virtual machine.
Convert to Template	Convert this virtual machine to a template.
Delete all Snapshots	Remove all snapshots for a virtual machine.
Delete Most Recent Snapshot	Removes a virtual machine's most recent snapshot.
Delete VM from Disk	Remove the virtual machine from disk.
Disconnect All CD-ROM Drives for Virtual Machine	Disconnect all the CD-ROM drives for the virtual machine.
Disconnect All Floppy Drives for Virtual Machine	Disconnect all the floppy drives for the virtual machine.
Disconnect All Floppy and CD-ROM Drives for Virtual Machine	Disconnect all of the floppy and CD-ROM drives for virtual machine.
Execute an external script	Run an external script.
Generate Audit Event	Write an entry to the audit log and to the VMDB.
Generate log message	Write an entry to the CloudForms Management Engine log.
Initiate SmartState Analysis for Host	Start a SmartState Analysis for a host.
Initiate SmartState Analysis for VM	Start a SmartState Analysis for a virtual machine.
Mark as Non-Compliant	Used with compliance policies. Mark resource as non-compliant. (Compliance status is viewable in summary screens.)
Prevent current event from proceeding	Stop the current event from continuing.
Put Virtual Machine Guest OS in Standby	Put the virtual machines operating system in standby mode.
Raise Automation Event	Used with CloudForms Management Engine automate.
Refresh data from vCenter	Perform a refresh of the vCenter.
Remove Virtual Machine from Inventory	Take the virtual machine out of inventory.
Retire Virtual Machine	Retire the virtual machine. (It will remain in inventory, but cannot be started.)
Shutdown Virtual Machines Guest OS	Shut down the virtual machine's operating system.

Action	Description
Start Virtual Machine	Power on the virtual machine.
Stop Virtual Machine	Power off the virtual machine.
Suspend Virtual Machine	Suspend the virtual machine.

5.1. Custom Actions

You can create a custom action using the CloudForms Management Engine console. Enter a description and action type. Procedures for each type of action are shown in the sections below. When you create a policy, you can associate actions with specific events.

Table 5.2. Custom Actions and Descriptions

Custom Action	Description
Assign Profile to Analysis Task	When initiating a Smart State Analysis event, you can assign a specific analysis profile.
Create a Snapshot	Creates a snapshot with a name that you provide.
Delete Snapshots by Age	Removes snapshots based on how old they are.
Evaluate Alerts	Checks for alerts. This is required for the alert to be delivered.
Inherit Parent Tags	Assigns tags from the parent cluster, host, datastore, or resource pool.
Invoke a Custom Automation	For use with CloudForms Management Engine automate.
Reconfigure CPUs	Reconfigure the number of CPUs for a virtual machine to the number you specify.
Reconfigure Memory	Reconfigure the amount of memory for a virtual machine to the amount you specify.
Remove Tags	Removes tags from the resource.
Send an E-mail	Send an email to an address that you provide. This type of action can be used in an alert.
Send an SNMP trap	Send an SNMP (Simple Network Management Protocol) trap to the host you specify. This type of action can be used for an alert.
Set a Custom Attribute in vCenter	Set the value of a custom attribute in vCenter.
Tag	Assign a company tag that you specify to a virtual machine.

5.1.1. Creating an Assign Profile to Analysis Task Action

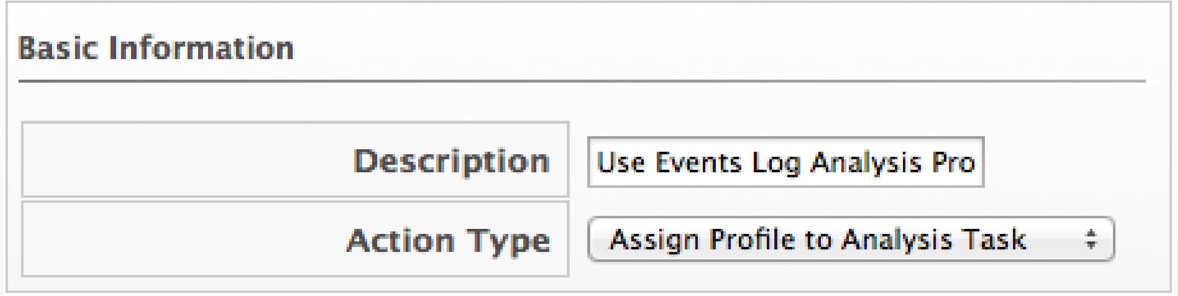
Use this action for assigning specific analysis profiles to virtual machines. You must create an analysis profile before assigning it to an action. You can only assign this action to an analysis start event. See the *CloudForms Management Engine Settings and Operations Guide* for information on how to create analysis profiles.

Procedure 5.1. To Create an Assign Profile to Analysis Task Action

1. Navigate to **Control** → **Explorer**.

2. Click the **Actions** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Action**).

3. Type in a **Description** for the **Action Type**.



Basic Information

Description: Use Events Log Analysis Pro

Action Type: Assign Profile to Analysis Task

4. Select **Assign Profile to Analysis Task** from **Action Type**.

5. Select a profile from the **Analysis profiles**.

6. Click **Add**.

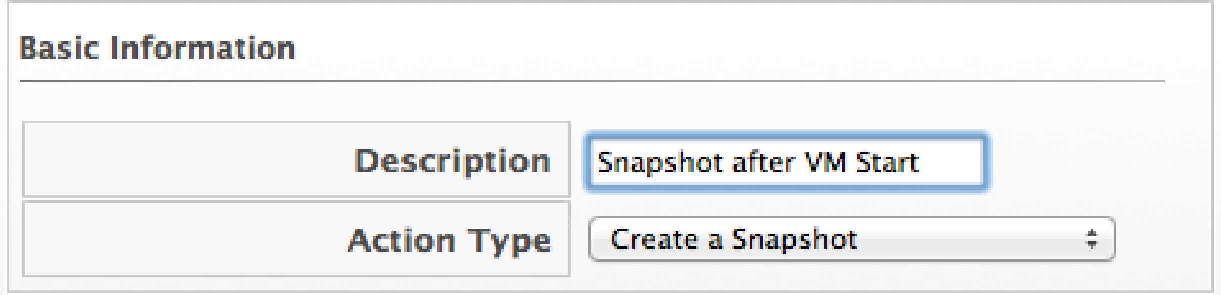
5.1.2. Creating a Snapshot Action

Procedure 5.2. To Create a Snapshot Action

1. Navigate to **Control** → **Explorer**.

2. Click the **Actions** accordion, then click ⚙ (**Configuration**), ➕ (**Add a new Action**).

3. Type in a **Description** for the action.



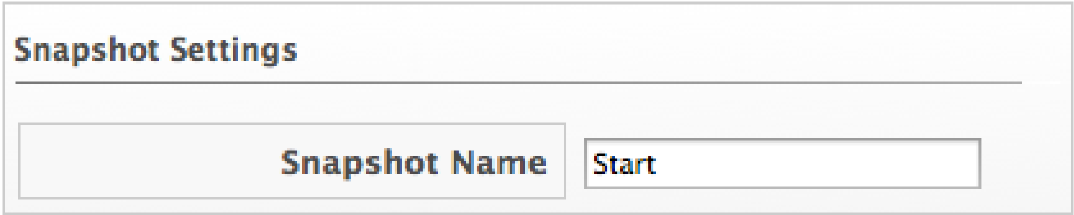
Basic Information

Description: Snapshot after VM Start

Action Type: Create a Snapshot

4. Select **Create a Snapshot** from **Action Type**.

5. Type in a **Snapshot Name**.



Snapshot Settings

Snapshot Name: Start

6. Click **Add** when you are finished.

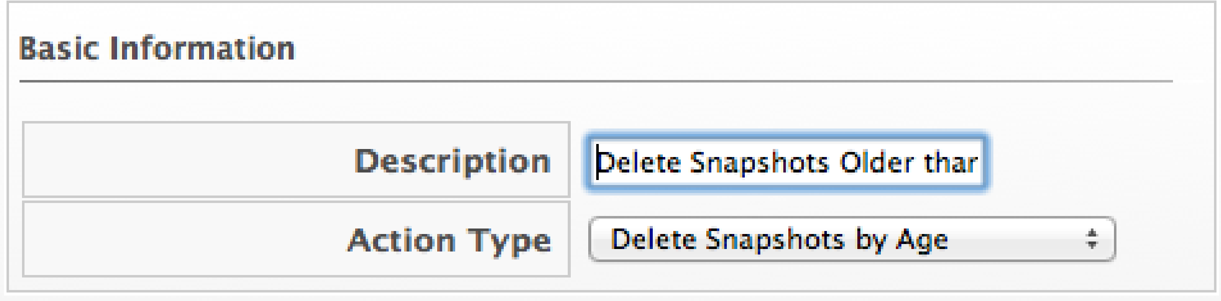
5.1.3. Deleting Snapshots by Age

Procedure 5.3. To Delete Snapshots by Age

1. Navigate to **Control** → **Explorer**.

2. Click the **Actions** accordion, then click ⚙ (**Configuration**), + (**Add a new Action**).

3. Type in a **Description** for the action.



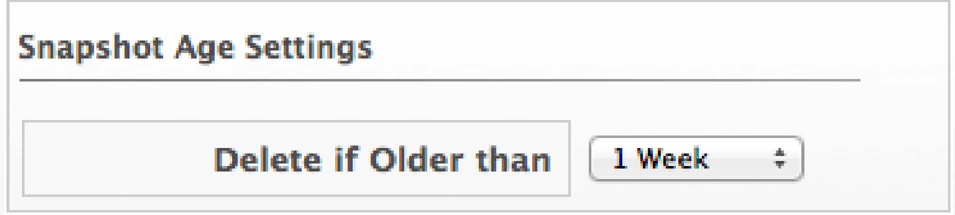
Basic Information

Description: Delete Snapshots Older thar

Action Type: Delete Snapshots by Age

4. Select **Delete Snapshots by Age** from **Action Type**.

5. Select the age of snapshots to delete.



Snapshot Age Settings

Delete if Older than: 1 Week

6. Click **Add**.

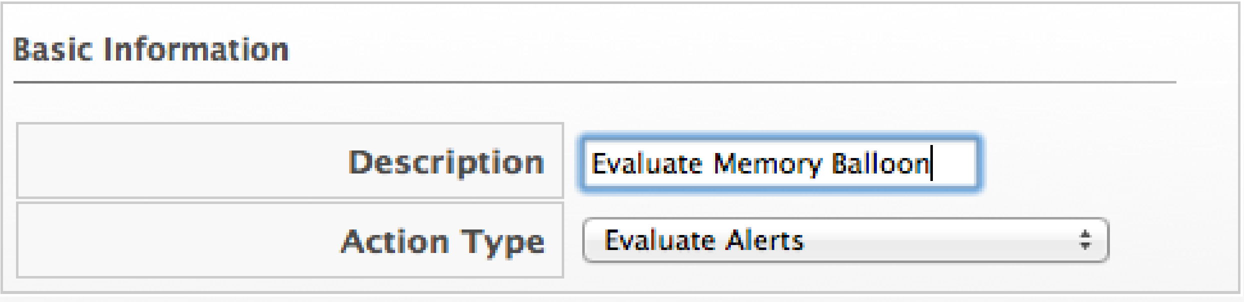
5.1.4. Evaluating an Alert

Procedure 5.4. To Evaluate an Alert

1. Navigate to **Control** → **Explorer**.

2. Click the **Actions** accordion, then click ⚙ (**Configuration**), + (**Add a new Action**).

3. Type in a **Description** for the action.



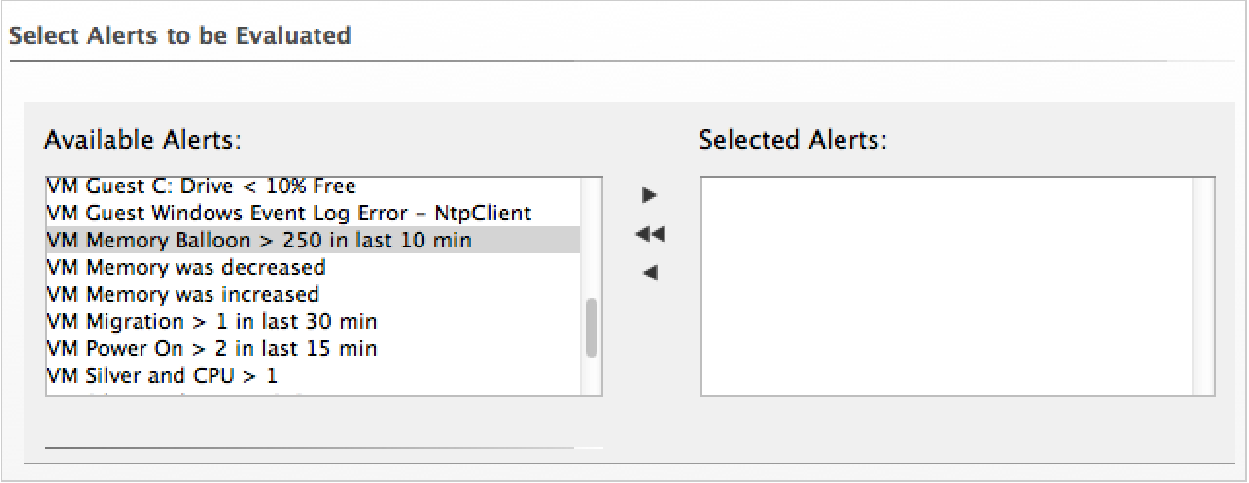
Basic Information

Description: Evaluate Memory Balloon

Action Type: Evaluate Alerts

4. Select **Evaluate Alerts** from **Action Type**.

5. Select the alerts to be evaluated and click ▶ (Move selected Alerts into this Action). Use the **Ctrl** key to select multiple alerts.



Select Alerts to be Evaluated

Available Alerts:

- VM Guest C: Drive < 10% Free
- VM Guest Windows Event Log Error - NtpClient
- VM Memory Balloon > 250 in last 10 min
- VM Memory was decreased
- VM Memory was increased
- VM Migration > 1 in last 30 min
- VM Power On > 2 in last 15 min
- VM Silver and CPU > 1

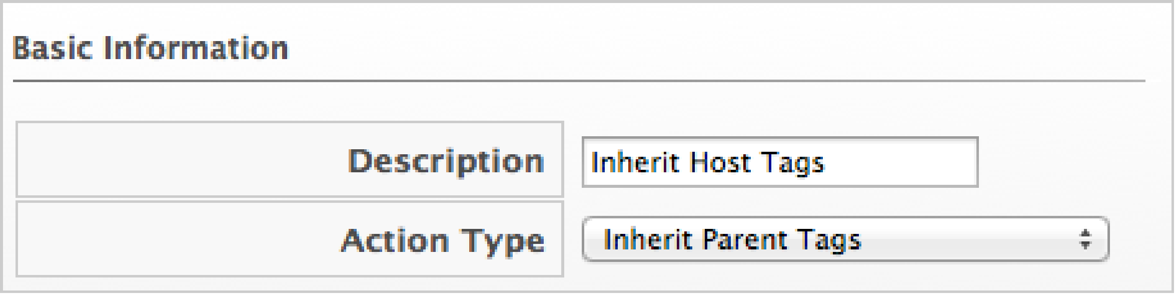
Selected Alerts:

6. Click **Add**.

5.1.5. Creating an Inherit Tag Action

Procedure 5.5. To Create an Inherit Tag Action

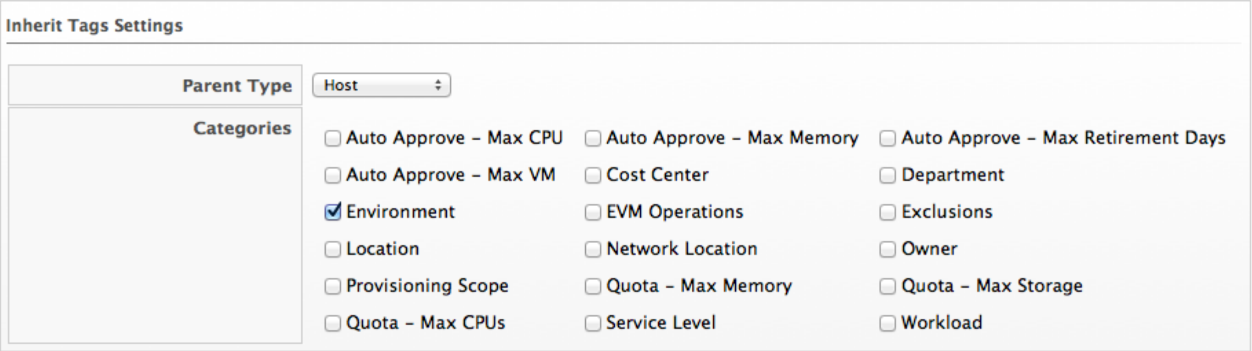
1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, and click ⚙ (**Configuration**), + (**Add a new Action**).
3. Type in a **Description** for the action.



Basic Information

Description	Inherit Host Tags
Action Type	Inherit Parent Tags

4. Select **Inherit Parent Tag** from **Action Type**.
5. Select the type of parent item to inherit from in **Parent Type**.
6. Check all categories that you want inherited.



Inherit Tags Settings

Parent Type: Host

Categories:

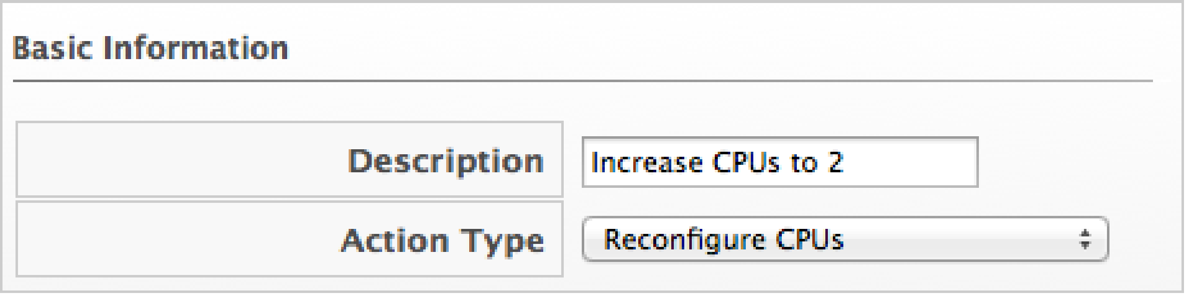
☐ Auto Approve - Max CPU	☐ Auto Approve - Max Memory	☐ Auto Approve - Max Retirement Days
☐ Auto Approve - Max VM	☐ Cost Center	☐ Department
☑ Environment	☐ EVM Operations	☐ Exclusions
☐ Location	☐ Network Location	☐ Owner
☐ Provisioning Scope	☐ Quota - Max Memory	☐ Quota - Max Storage
☐ Quota - Max CPUs	☐ Service Level	☐ Workload

7. Click **Add**.

5.1.6. Creating a CPU Reconfigure Action

Procedure 5.6. To Create a CPU Reconfigure Action

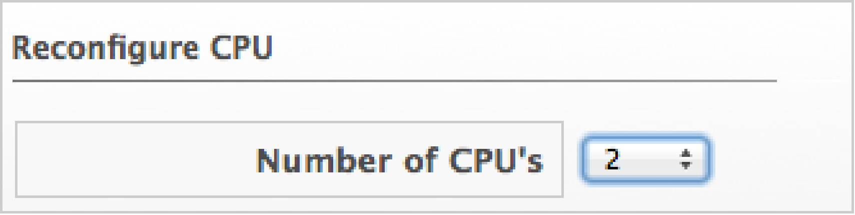
1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click ⚙ (**Configuration**), + (**Add a new Action**).
3. Type in a **Description** for the action.



Basic Information

Description	Increase CPUs to 2
Action Type	Reconfigure CPUs

4. Select **Reconfigure CPUs** from **Action Type**.
5. Select a number from **Number of CPUs**.



Reconfigure CPU

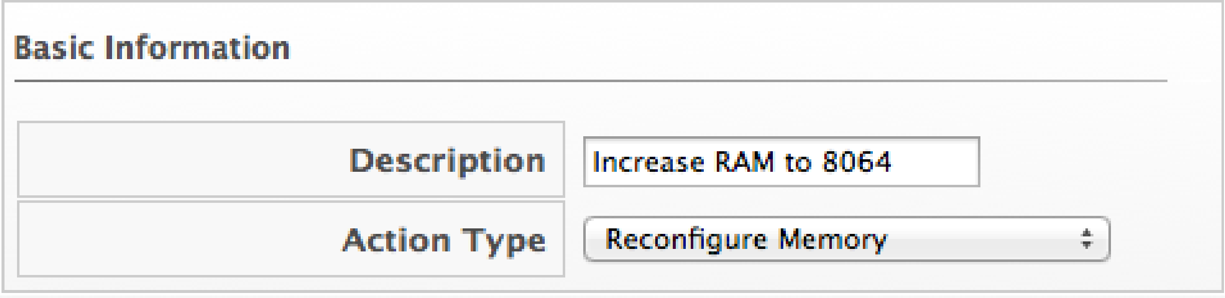
Number of CPU's	2

6. Click **Add**.

5.1.7. Creating a Memory Reconfigure Action

Procedure 5.7. To Create a Memory Reconfigure Action

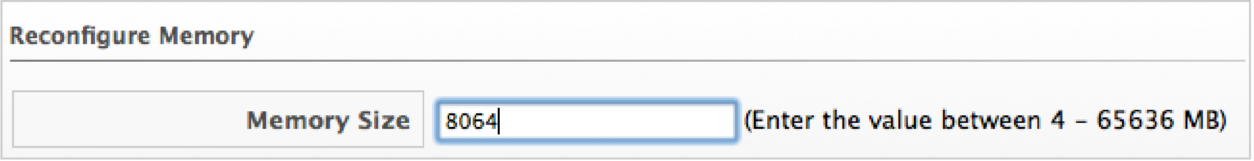
1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click ⚙ (**Configuration**), + (**Add a new Action**).
3. Type in a **Description** for the action.



Basic Information

Description	Increase RAM to 8064
Action Type	Reconfigure Memory

4. Select **Reconfigure Memory** from **Action Type**.
5. Type in a new value for **Memory Size**.



Reconfigure Memory

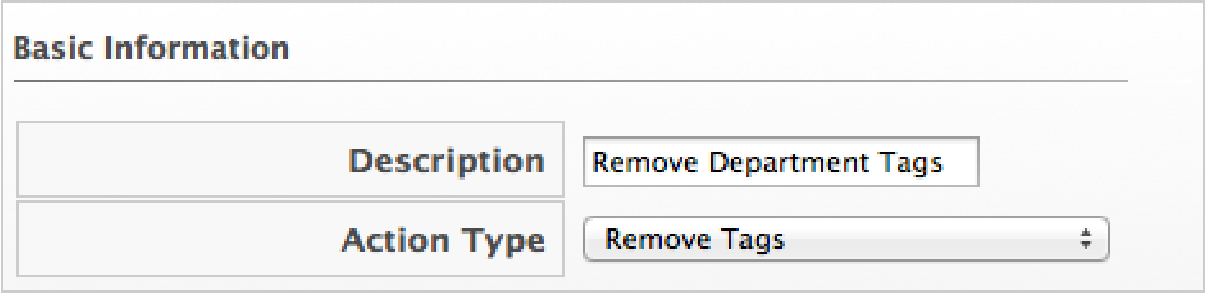
Memory Size: 8064 (Enter the value between 4 – 65636 MB)

6. Click **Add**.

5.1.8. Creating a Remove Tag Action

Procedure 5.8. To Create a Remove Tag Action

1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Action**).
3. Type in a **Description** for the action.

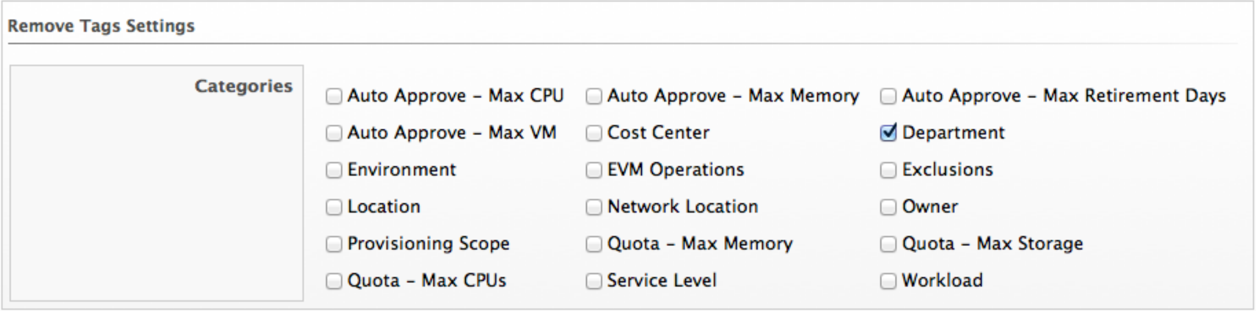


Basic Information

Description: Remove Department Tags

Action Type: Remove Tags

4. Select **Remove Tags** from **Action Type**.
5. Check the category of tags you want to remove.



Remove Tags Settings

Categories

□ Auto Approve - Max CPU
□ Auto Approve - Max Memory
□ Auto Approve - Max Retirement Days
□ Auto Approve - Max VM
□ Cost Center
☑ Department
□ Environment
□ EVM Operations
□ Exclusions
□ Location
□ Network Location
□ Owner
□ Provisioning Scope
□ Quota - Max Memory
□ Quota - Max Storage
□ Quota - Max CPUs
□ Service Level
□ Workload

6. Click **Add**.

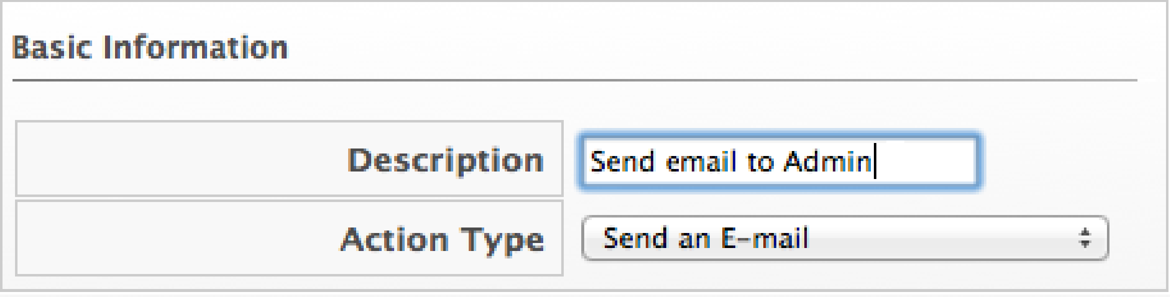
5.1.9. Creating an E-mail Action

Note

To be able to send any emails from the CloudForms Management Engine server, you must have the notifier server role enabled and have defined settings for SMTP email in Configuration-Operations-Server. For further information regarding SMTP, see the Settings and Operations guide.

Procedure 5.9. To Create an E-mail Action

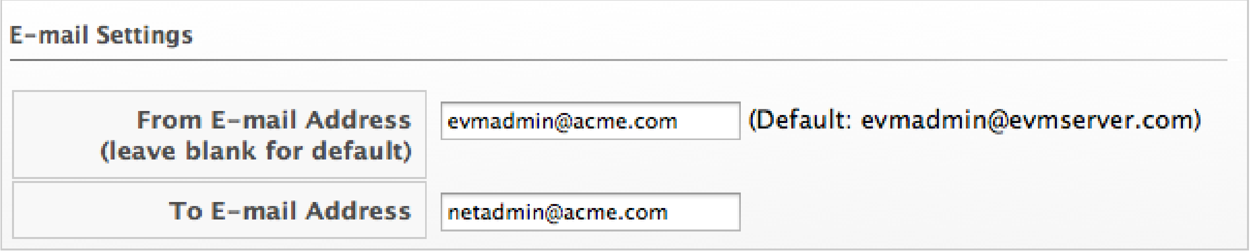
1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click ⚙ (**Configuration**), + (**Add a new Action**).
3. Type in a **Description** for the action.



Basic Information

Description	Send email to Admin
Action Type	Send an E-mail

4. Select **Send an E-mail** from **Action Type**.
5. Type in a **From E-mail Address** and **To E-mail Address**.



E-mail Settings

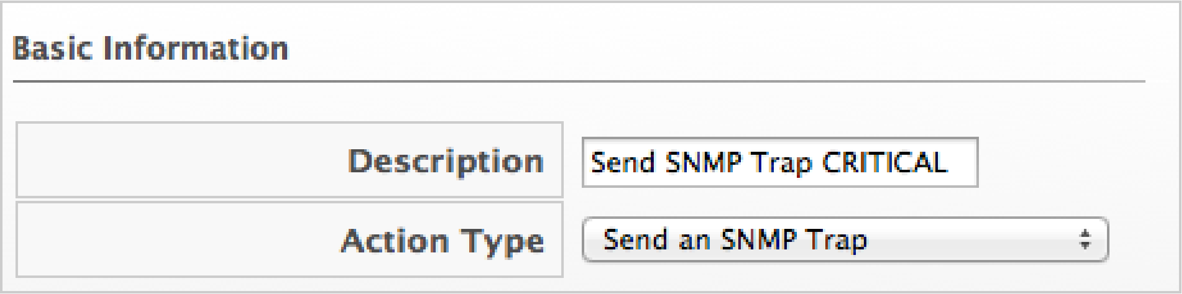
From E-mail Address (leave blank for default)	evmadmin@acme.com	(Default: evmadmin@evmserver.com)
To E-mail Address	netadmin@acme.com	

6. Click **Add**.

5.1.10. Creating an SNMP Action

Procedure 5.10. To Create an SNMP Action

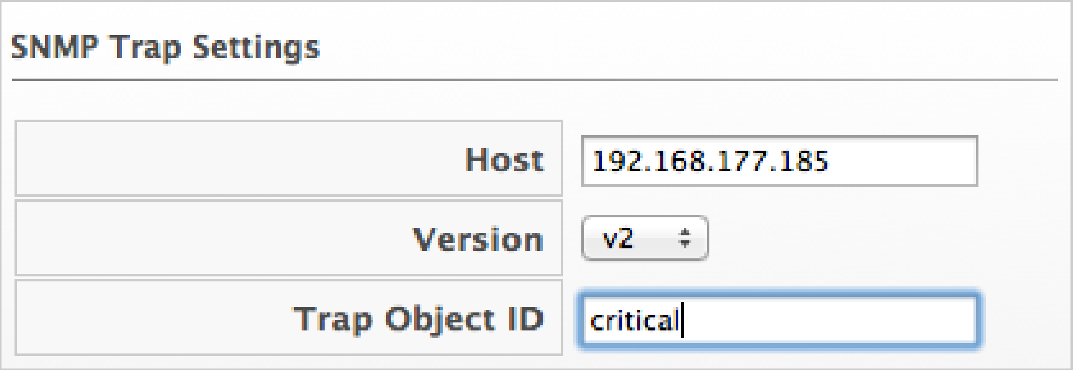
1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click ⚙ (**Configuration**), + (**Add a new Action**).
3. Type in a **Description** for the action.



Basic Information

Description	Send SNMP Trap CRITICAL
Action Type	Send an SNMP Trap

4. Select **Send an SNMP Trap** from **Action Type**.


SNMP Trap Settings

Host	192.168.177.185
Version	v2
Trap Object ID	critical

5. Type in the IP for the host to send the trap to, select the version of SNMP that you are using, and type in the Trap Object ID. Type in multiple hosts if you require the trap sent to multiple SNMP hosts.

   - If using SNMP V1, you are prompted for a Trap Number. Type 1, 2, or 3, based on the appropriate Suffix Number from table below.

   - If using SNMP V2, you are prompted for a Trap Object ID. Type info, warning, or critical, based on the table below.

     Trap Object ID and Suffix Number

Object ID	Suffix Number Added to PEN	PEN with the Suffix Added
info	1	1.3.6.1.4.1.33482.1
warn, warning	2	1.3.6.1.4.1.33482.2
crit, critical, error	3	1.3.6.1.4.1.33482.3

6. Type in the variables that you require in your message.

7. Click **Add**.

Note

When adding an SNMP action, be sure to set it as asynchronous.

5.1.11. Creating a Set Custom Attribute Action

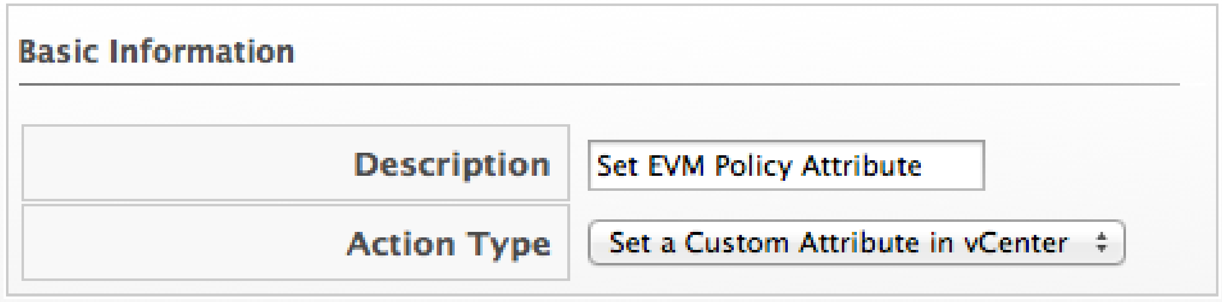
The custom attribute must already exist in vCenter. See the vCenter documentation for instructions. In this example, an attribute called CloudForms Management Engine policy already exists.

Procedure 5.11. To Create a Set Custom Attribute Action

1. Navigate to **Control** → **Explorer**.

2. Click the **Actions** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Action**).

3. Type in a **Description** for the action.

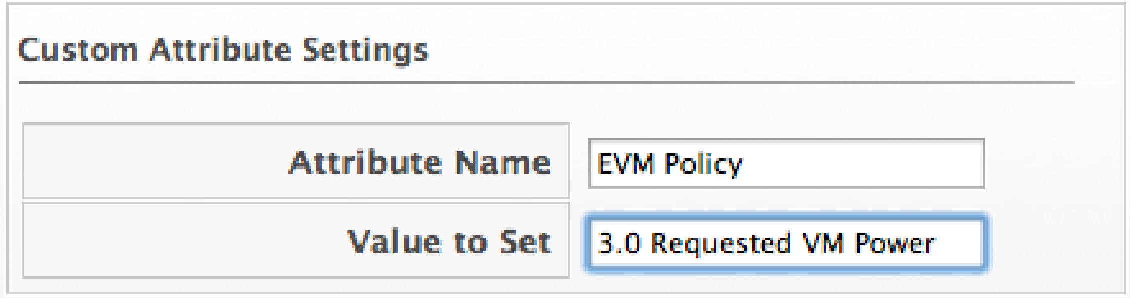


Basic Information

Description	Set EVM Policy Attribute
Action Type	Set a Custom Attribute in vCenter

4. Select **Set a Custom Attribute in vCenter** from **`Action Type`**.

5. Type in the **`Attribute Name`** and **`Value to Set`**.



Custom Attribute Settings

Attribute Name	EVM Policy
Value to Set	3.0 Requested VM Power

6. Click **Add**.

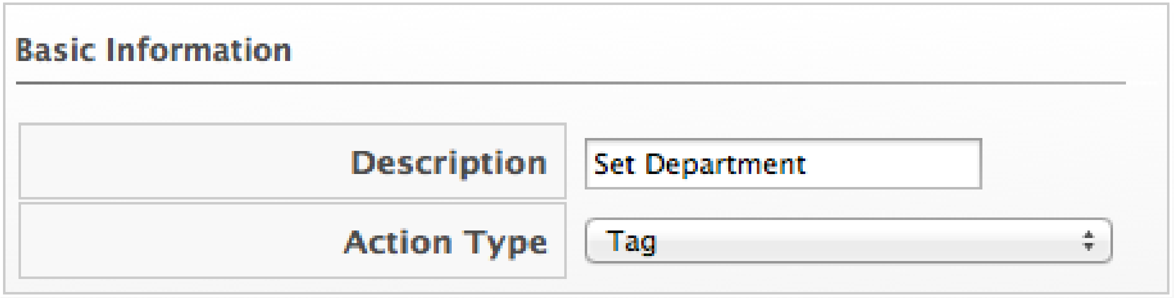
5.1.12. Creating a Tag Action

Procedure 5.12. To Create a Tag Action

1. Navigate to **Control** → **Explorer**.

2. Click the **Actions** accordion, then click ⚙ (**`Configuration`**), ✚ (**`Add a new Action`**).

3. Type in a description for the action.

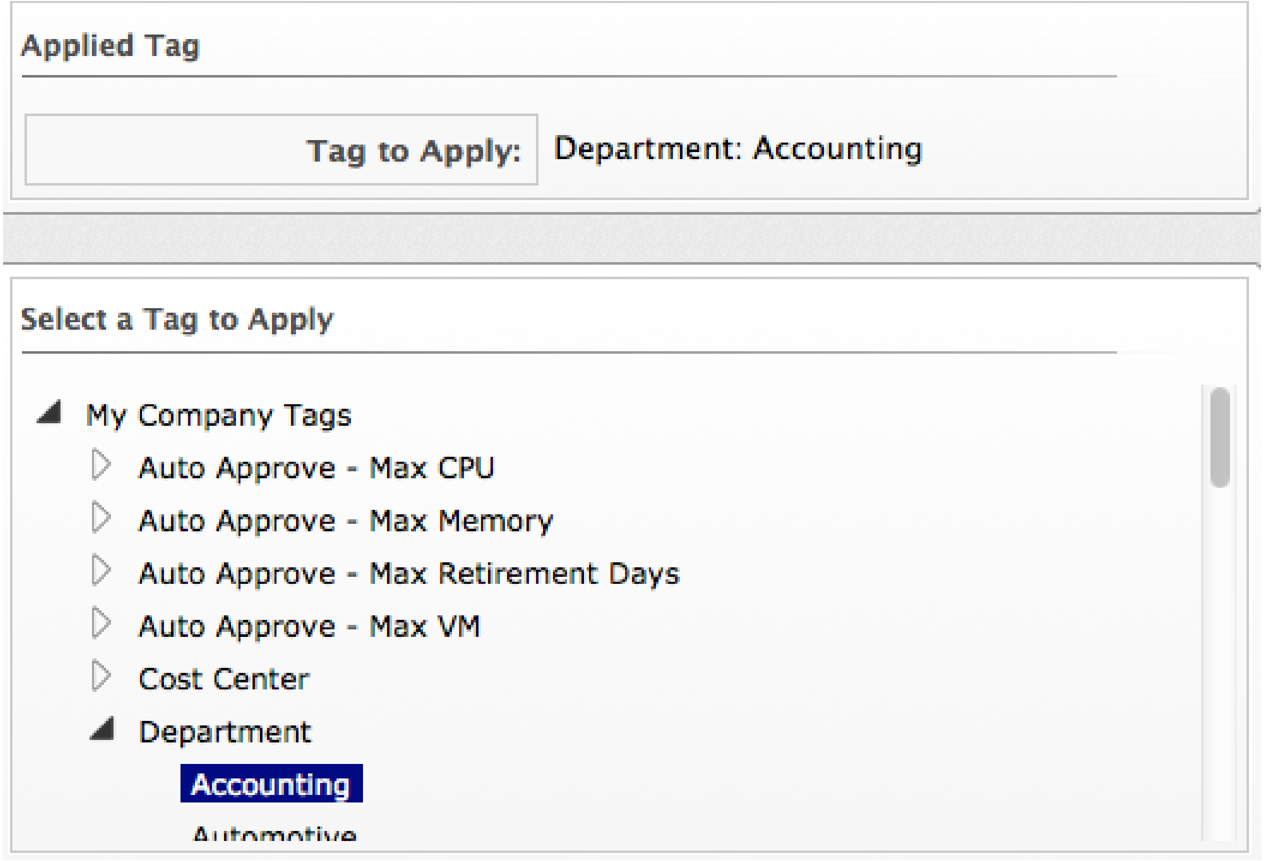


Basic Information

Description	Set Department
Action Type	Tag

4. Select **Tag** from **`Action Type`**.

5. Click on the appropriate tag to apply from the list provided.



Applied Tag

Tag to Apply: Department: Accounting

Select a Tag to Apply

6. Click **Add**.

5.2. Editing an Action

Edit an action to modify its properties. You cannot edit any of the default actions supplied with CloudForms Management Engine. Only actions that you create can be changed.

Note that when you view an action, you can see what policies it has been assigned to.

Procedure 5.13. To Edit an Action

1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click on the action you need to edit.
3. Click ⚙ (**Configuration**), ✎ (**Edit this Action**) on the detail view of the action.
4. Make any required changes.
5. Click **Save**.

Result:

The action is modified and can be added to a policy. If the action is already party of a policy, the policy is automatically updated.

5.3. Deleting an Action

Delete unused actions to keep your environment uncluttered. You cannot delete default actions or actions that are currently assigned to a policy. The delete button is unavailable if the action is in use.

Procedure 5.14. To Delete an Action

1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, click on the action you need to remove.
3. Click ⚙ (**Configuration**), 🗑 (**Delete this Action**) on the detail view of the tree.
4. Click **OK** to confirm.

Chapter 6. Policy Profiles

6.1. Creating Policy Profiles

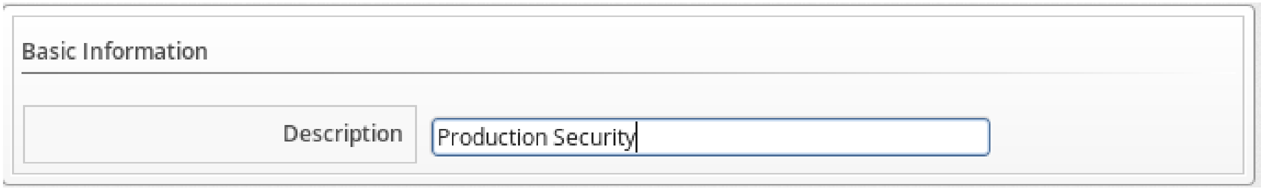
Policy profiles are groups of policies that you need to use at the same time. A policy profile can have one or more policies. Policy profiles can be assigned to either a host or a virtual machine.

Procedure 6.1. To Create a Policy Profile

1. Navigate to **Control** → **Explorer**.

2. Click on the **Policy Profiles** accordion, then click ⚙ (**Configuration**), then ✚ (**Add a New Policy Profile**).

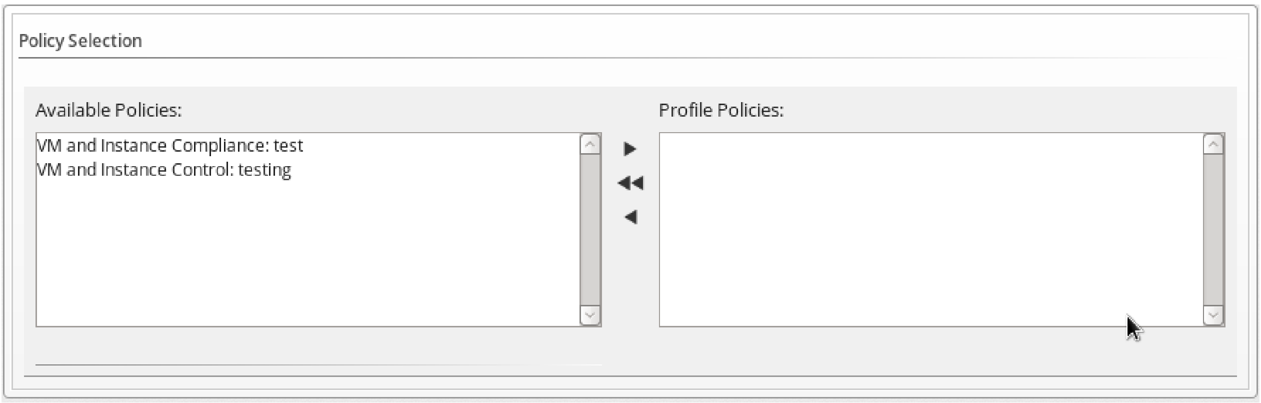
3. In the **Basic Information** area, type in a unique description for the policy profile.



Basic Information

Description: Production Security

4. From **Available Policies** in the **Policy Selection** area select all the policies you need to apply to this policy profile. Use the **Ctrl** key to select multiple policies.



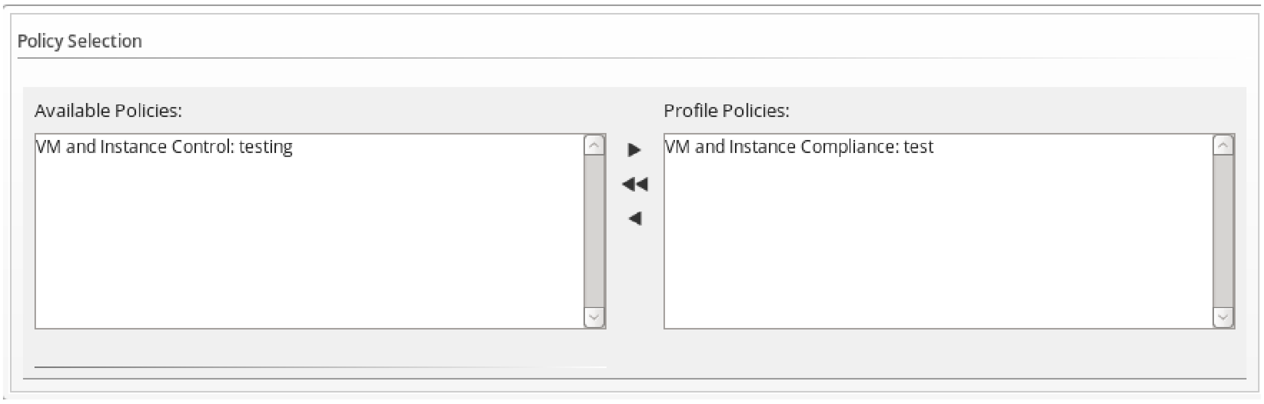
Policy Selection

Available Policies:

VM and Instance Compliance: test
VM and Instance Control: testing

Profile Policies:

5. Click ▶ to add the Policies.



Policy Selection

Available Policies:

VM and Instance Control: testing

Profile Policies:

VM and Instance Compliance: test

6. Add to the **Notes** area if required.

7. Click **Add**.

Result:

The policy profile is added. You can now assign the policy profile to providers, hosts, and repositories. In addition, you can verify that the virtual machine complies with the policy profile using the *Resultant Set of Policy* feature.

6.2. Deleting a Policy Profile

Remove policy profiles that you no longer need. This does not remove the policies associated with the policy profile.

Procedure 6.2. To Delete a Policy Profile

1. Navigate to **Control** → **Explorer**.
2. Click on the **Policy Profile** accordion, then click the policy profile you want to remove.
3. Click ⚙ (**`Configuration`**), 🗑 (**`Remove this Policy Profile`**).
4. Click **`OK`** to confirm.

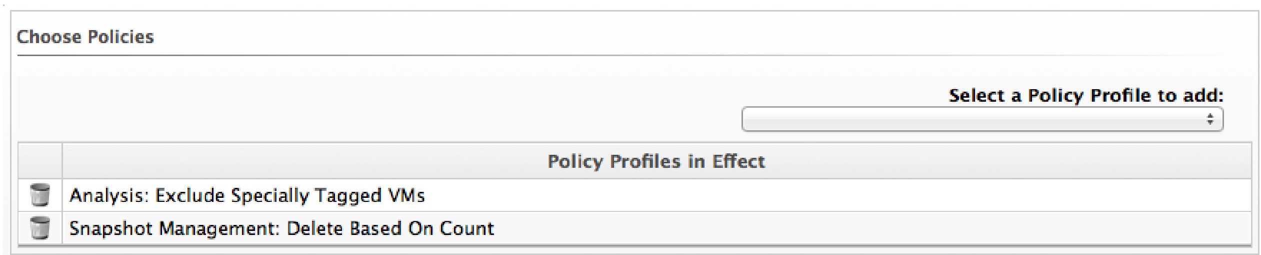
6.3. Simulating Policy

Before assigning a policy profile to a virtual machine, use the CloudForms Management Engine controls policy simulation feature to determine if a virtual machine passes a policy profile.

6.3.1. Simulating Policy Profiles on Virtual Machines

Procedure 6.3. To Simulate Policy Profiles on Virtual Machines

1. Navigate to **Infrastructure** → **Virtual Machines**, select the virtual machines you need to evaluate.
2. Click 🛡 (**`Policy`**), and then click ? (**`Policy Simulation`**).
3. From the **`Select a Policy Profile to add`** dropdown, click the policy you need to apply to the selected virtual machines.



Choose Policies

Select a Policy Profile to add:

	Policy Profiles in Effect
🗑	Analysis: Exclude Specially Tagged VMs
🗑	Snapshot Management: Delete Based On Count

4. The virtual machine thumbnail displays in the **`Policy Simulation`** area.
   - A check sign in the lower right quadrant of the virtual thumbnail shows that the virtual machine passes policy.
   - A minus sign in the lower right quadrant of the virtual thumbnail shows that the virtual machine fails policy.

5. Click on a virtual machine in the **Policy Simulation** area to see its details.

6. Expand a policy profile by clicking on it to see its member policies and the status of the conditions.

   - Check ***Show out of scope items*** to show all conditions, whether or not the virtual machine passes the scope part of the condition. Uncheck it to hide conditions where the scope part fails.
   - Next to ***Show policies***, check ***Successful*** to show policies that are passed and check ***Failed*** to see the policies that have failed. The default is to show both.
   - Items in green text passed the condition.
   - Items in red text failed the condition.
   - Items in red italics failed the condition, but do not change the outcome of the scope.

Result:

If you evaluate multiple policy profiles, you can see both policy profiles and a tree expanding down to their conditions.

6.4. Assigning Policy Profiles

After creating your policy profiles, you are ready to evaluate and assign them. Policy profiles are assigned to virtual machines, providers, clusters, hosts, resource pools, and repositories. Policies within a profile run either on a Host or virtual machine based on the type of policy created.

- Assign a policy profile to a virtual machine to apply the policy profile to a specific virtual machine, independent of its related host, provider, or repository.
- Assign a policy profile to a provider to apply the policy profile to all virtual machines or hosts registered to that provider.
- Assign a policy profile to a cluster to apply the policy profile to all virtual machines or hosts assigned to that cluster.
- Assign a VM policy profile to a host to apply the policy profile to that specific host or all virtual machines registered to that Host.
- Assign a VM policy profile to a resource pool to apply the policy profile to all virtual machines or hosts assigned to that resource pool.
- Assign a VM policy profile to a repository to apply the policy profile to all virtual machines registered to that repository.

6.4.1. Assigning Policy Profiles to a Provider

Procedure 6.4. To Assign Policy Profiles to a Provider

1. Navigate to **Infrastructure** → **Providers**, verify the provider you need to assign the policy profiles to.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, you can click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Check the policy profiles you require to apply to the provider. It turns blue to show its assignment state has changed.

5. Click **Save**.

6.4.2. Removing Policy Profiles from a Provider

Procedure 6.5. To Remove Policy Profiles from a Provider

1. Navigate to **Infrastructure** → **Providers**, check the providers you want to remove the policy profile from.

2. Click (**Policy**), and then click (**Manage Policies**).

3. Uncheck the policy profile you need to remove. It turns blue to show that its assignment state has changed.

4. Click **Save**.

6.4.3. Assigning Policy Profiles to a Cluster

Procedure 6.6. To Assign Policy Profiles to a Cluster

1. Navigate to **Infrastructure** → **Clusters**, check the clusters you need to assign policy profiles to.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, you can click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Check the policy profiles you need to apply to the cluster. It turns blue to show its assignment state has changed.

5. Click **Save**.

6.4.4. Removing Policy Profiles from a Cluster

Procedure 6.7. To Remove Policy Profiles from a Cluster

1. Navigate to **Infrastructure** → **Clusters**, check the clusters you need to remove the policy profiles from.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, you can click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Uncheck the policy profiles you need to remove. It turns blue to show that its assignment state has changed.

5. Click **Save**.

6.4.5. Assigning Policy Profiles to a Host

Procedure 6.8. To Assign Policy Profiles to a Host

1. Navigate to **Infrastructure** → **Hosts**, check the hosts you need to assign policy profiles to.
2. Click (**Policy**), and then click (**Manage Policies**).
3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.
4. Check the policy profiles you need to apply to the host. It turns blue to show its assignment state has changed.
5. Click **Save**.

6.4.6. Removing Policy Profiles from a Host

Procedure 6.9. To Remove Policy Profiles from a Host

1. Navigate to **Infrastructure** → **Hosts**, check the hosts you need to remove the policy profiles from.
2. Click (**Policy**), and then click (**Manage Policies**).
3. Uncheck the policy profiles you need to remove. It turns blue to show that its assignment state has changed.
4. Click **Save**.

6.4.7. Assigning Policy Profiles to a Virtual Machine

Procedure 6.10. To assign policy profiles to a virtual machine

1. Navigate to **Infrastructure** → **Virtual Machines**, check the virtual machines you need to assign policy profiles to.
2. Click (**Policy**), and then click (**Manage Policies**).
3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.
4. Check the policy profiles you need to apply to the host. It will turn blue to show that its assignment state has changed.
5. Click **Save**.

6.4.8. Removing Policy Profiles from a Virtual Machine

Procedure 6.11. To Remove Policy Profiles from a Virtual Machine

1. Navigate to **Infrastructure** → **Virtual Machines**, check the virtual machines you want to remove the policy profile from.

2. Click 🛡 (**Policy**), and then click 🛡 (**Manage Policies**).
3. Uncheck the policy profile you need to remove. It turns blue to show that its assignment state has changed.
4. Click **Save**.

6.4.9. Assigning Policy Profiles to a Resource Pool

Procedure 6.12. To Assign Policy Profiles to a Resource Pool

1. Navigate to **Infrastructure** → **Resource Pools**, check the resource pools you need to assign policy profiles to.
2. Click 🛡 (**Policy**), and then click 🛡 (**Manage Policies**).
3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.
4. Click the policy profiles you need to apply to the resource pools. It turns blue to show its assignment state has changed.
5. Click **Save**.

6.4.10. Removing Policy Profiles from a Resource Pool

Procedure 6.13. To Remove Policy Profiles from a Resource Pool

1. Navigate to **Infrastructure** → **Resource Pools**, check the resource pools you need to remove the policy profiles from.
2. Click 🛡 (**Policy**), and then click 🛡 (**Manage Policies**).
3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.
4. Uncheck the policy profiles you need to remove. It turns blue to show that its assignment state has changed.
5. Click **Save**.

6.4.11. Assigning Policies to a Repository

Procedure 6.14. To Assign Policies to a Repository

1. Navigate to **Infrastructure** → **Repositories**, check the repositories you need to assign the policy profiles to.
2. Click 🛡 (**Policy**), and then click 🛡 (**Manage Policies**).
3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Check the policy profiles you need to apply to the provider. It turns blue to show its assignment state has changed.

5. Click **Save** to confirm.

6.4.12. Removing Policy Profiles from a Repository

Procedure 6.15. To Remove Policy Profiles from a Repository

1. Navigate to **Infrastructure** → **Repositories**, check the repositories you need to remove the policy profile from.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Uncheck the policy profile you need to remove. It turns blue to show that its assignment state has changed.

5. Click **Save**.

6.4.13. Assigning Policy Profiles to a Cloud Provider

Procedure 6.16. To Assign Policy Profiles to a Cloud Provider

1. Navigate to **Clouds** → **Providers**, check the provider you need to assign the policy profiles to.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Check the policy profiles you need to apply to the provider. The ones that are different from the previous setting will show in blue.

5. Click **Save**.

6.4.14. Removing Policy Profiles from a Cloud Provider

Procedure 6.17. To Remove Policy Profiles from a Cloud Provider

1. Navigate to **Clouds** → **Providers**, check the providers you need to remove the policy profile from.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Uncheck the policy profile you need to remove. It turns blue to show that its assignment state has changed.

5. Click **Save**.

6.4.15. Assigning Policy Profiles to an Instance

Procedure 6.18. To Assign Policy Profiles to an Instance

1. From **Clouds** → **Instances**, check the instances you want to assign policy profiles to.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Check the policy profiles you want to apply to the instances. It turns blue to show its assignment state has changed.

5. Click **Save**.

6.4.16. Removing Policy Profiles from an Instance

Procedure 6.19. To Remove Policy Profiles from an Instance

1. Navigate to **Clouds** → **Instances**, check the instances you need to remove the policy profile from.

2. Click (**Policy**), and then click (**Manage Policies**).

3. From the **Select Policy Profiles** area, click on the triangle next to a desired policy profile to expand it and see its member policies.

4. Uncheck the policy profile you need to remove. It turns blue to show that its assignment state has changed.

5. Click **Save**.

6.5. Disabling a Policy in a Policy Profile

You can disable one policy in a profile without removing it from the policy, perhaps for trouble shooting purposes or because the policy is not required temporarily.

Procedure 6.20. To Disable a Policy

1. Navigate to **Control** → **Explorer**.

2. Click the **Policies** accordion, then navigate to the policy that you need to disable or navigate to the policy from the policy profile.

3. Click (**Configuration**), (**Edit Basic Info, Scope, Notes**).

4. Uncheck **Active**.

5. Click **Save**.

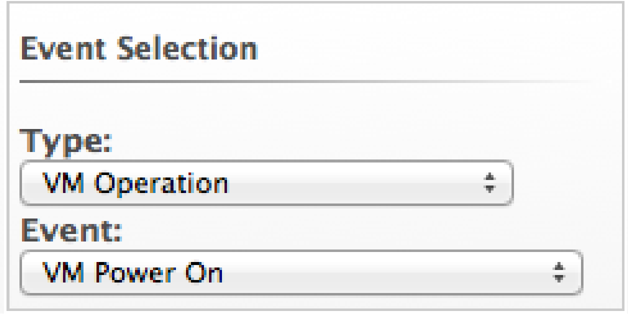
6.6. Viewing Policy Simulation - Resultant Set of Policy (RSOP)

After the Policy Profiles are assigned, you can see the final result of the resolution of all policies based on which Events occur. Based on the result, you can adjust your Policies. To view RSOP, go to the control area in the CloudForms Management Engine console.

Procedure 6.21. To View Policy Simulation (RSOP)

1. Navigate to **Control** → **Simulation**.

2. From the **`Event Selection`** area, select a type of event, and then the specific event you need the result for.

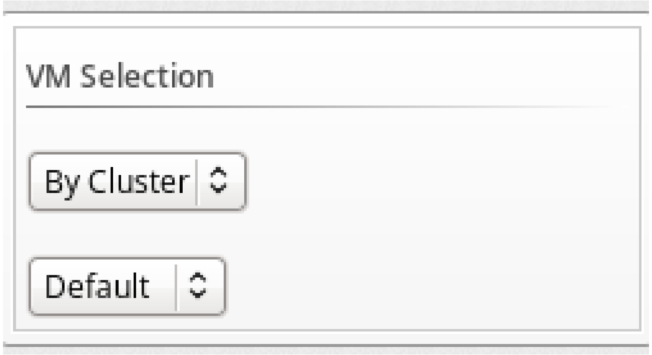


Event Selection

Type: VM Operation

Event: VM Power On

3. From the **`VM Selection`** area, select the virtual machine from a provider, cluster, host, or a single virtual machine.



VM Selection

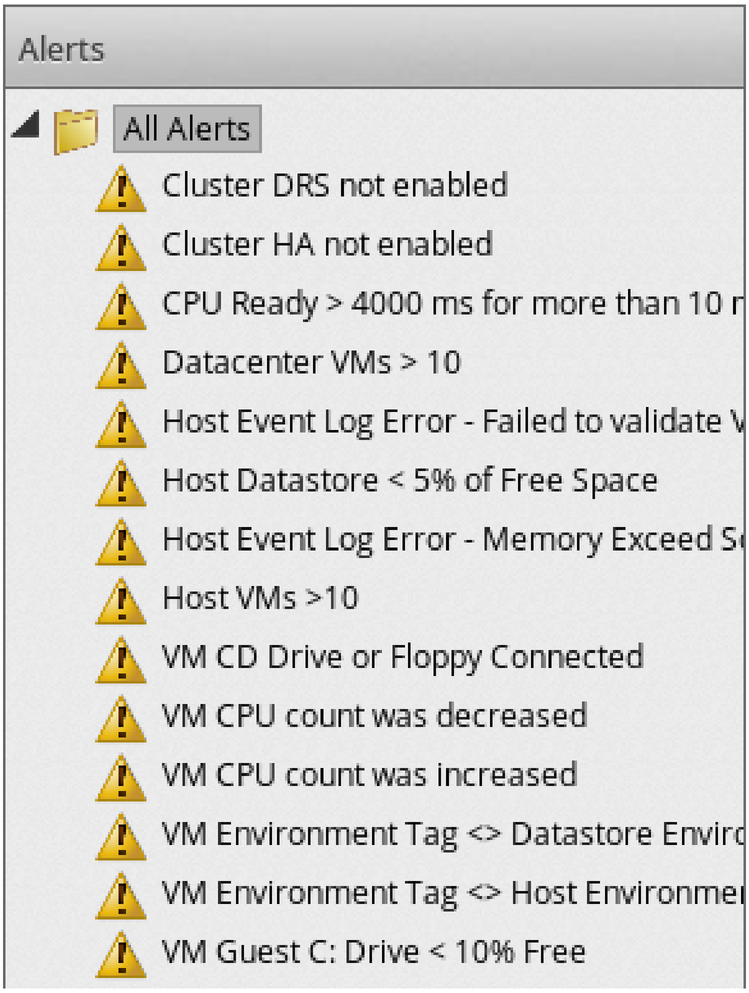
By Cluster

Default

4. Click **`Submit`**.

Chapter 7. Alerts

CloudForms Management Engine Alerts are used to notify administrators and monitoring systems on critical configuration changes and threshold limits in your virtual environment. The notification can take the form of an email or an SNMP trap. In addition, you can also invoke an automate process. CloudForms Management Engine provides you with some Alerts including Alerts specifically created for CloudForms Management Engine operations, but also enables you to create your own.



Alerts

- All Alerts
  - Cluster DRS not enabled
  - Cluster HA not enabled
  - CPU Ready > 4000 ms for more than 10 r
  - Datacenter VMs > 10
  - Host Event Log Error - Failed to validate V
  - Host Datastore < 5% of Free Space
  - Host Event Log Error - Memory Exceed S
  - Host VMs >10
  - VM CD Drive or Floppy Connected
  - VM CPU count was decreased
  - VM CPU count was increased
  - VM Environment Tag <> Datastore Enviro
  - VM Environment Tag <> Host Environme
  - VM Guest C: Drive < 10% Free

7.1. Notifier Server Role

CloudForms Management Engine also has a server role called Notifier specifically created for forwarding SNMP Traps and SMTP emails. If more than one CloudForms Management Engine server in a specific CloudForms Management Engine zone has this role, only one is active at a time.

> **Note**
>
> To be able to send an email from the CloudForms Management Engine Server, you must have the Notifier enabled. To enable this, you must have the **`EvmRole-administrator`** role.

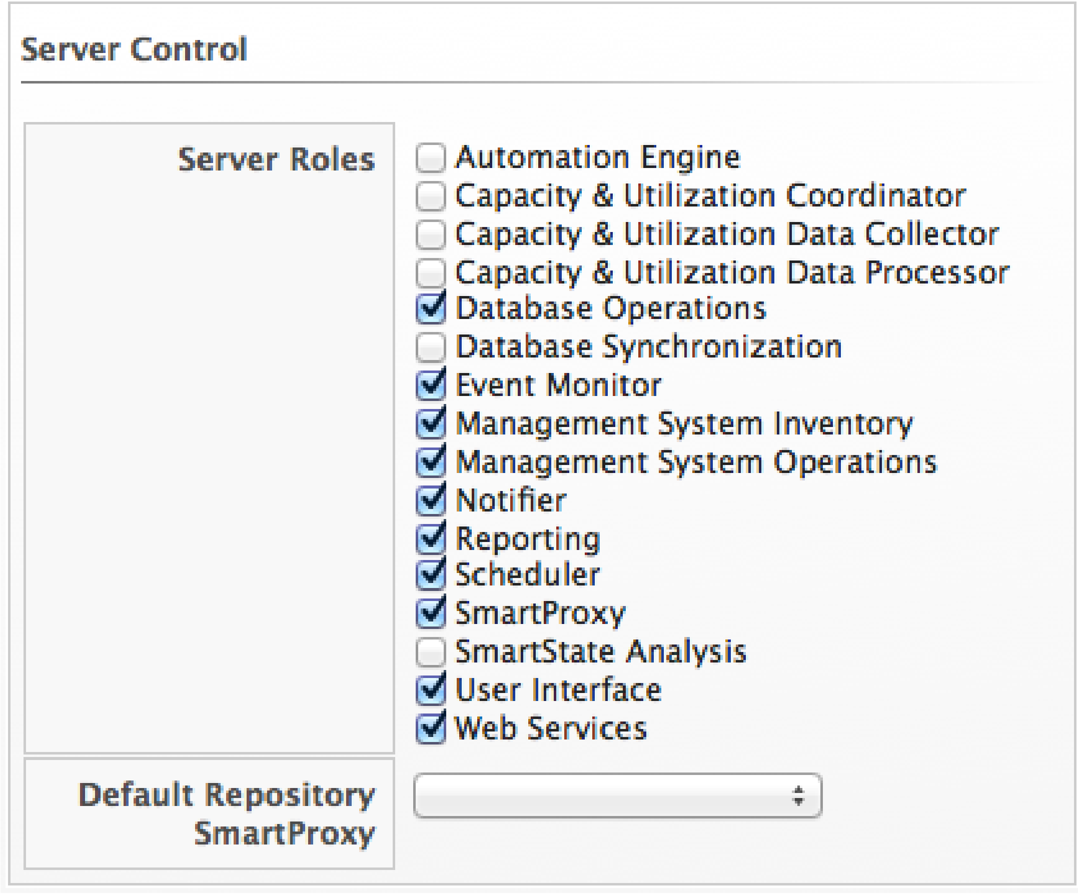
7.2. Assigning the Notifier Role

Procedure 7.1. To Assign the Notifier Role

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

2. Click the **Settings** accordion, and select the CloudForms Management Engine server.

3. From the **Server Control** tab, check the **Notifier** role.



Server Control

Server Roles
☐ Automation Engine
☐ Capacity & Utilization Coordinator
☐ Capacity & Utilization Data Collector
☐ Capacity & Utilization Data Processor
☑ Database Operations
☐ Database Synchronization
☑ Event Monitor
☑ Management System Inventory
☑ Management System Operations
☑ Notifier
☑ Reporting
☑ Scheduler
☑ SmartProxy
☐ SmartState Analysis
☑ User Interface
☑ Web Services

Default Repository SmartProxy

4. Click **Save**.

7.3. Creating an Alert

In this section, the basics of creating an Alert are described. Detailed instructions for the specific types of Alerts are given in the sections following.

Procedure 7.2. To Create an Alert

1. Navigate to **Control** → **Explorer**.

2. Click on the **Alerts** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Alert**).

   a. Type in a description for the alert.

   b. Check **Active** when you feel that the alert is ready to be enabled.

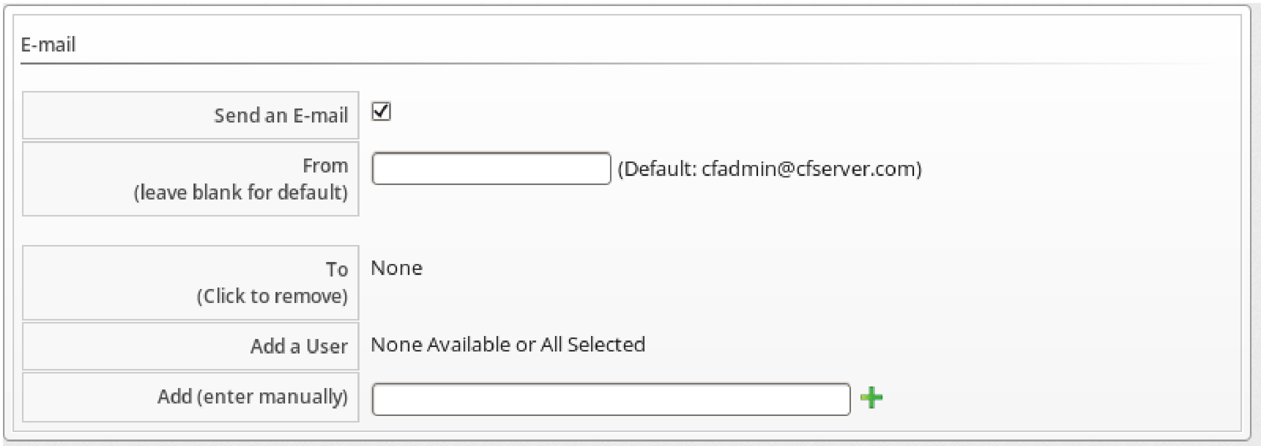
   c. From **Based On**, select the type of infrastructure item to base the alert on.

   d. The options shown in **What to Evaluate** change based on what you selected in **Based On**.

   e. In **Notification Frequency**, select how often you want to be notified if the event log threshold is reached.

3. The parameters available are based on the **What to Evaluate** selection. See the following sections for additional details on each alert type.

4. To send an email, check **Send an E-mail**. Parameters required for sending an email are displayed.



E-mail

Send an E-mail	☑
From (leave blank for default)	(Default: cfadmin@cfserver.com)
To (Click to remove)	None
Add a User	None Available or All Selected
Add (enter manually)	+

   a. In **From**, type in the sending email.

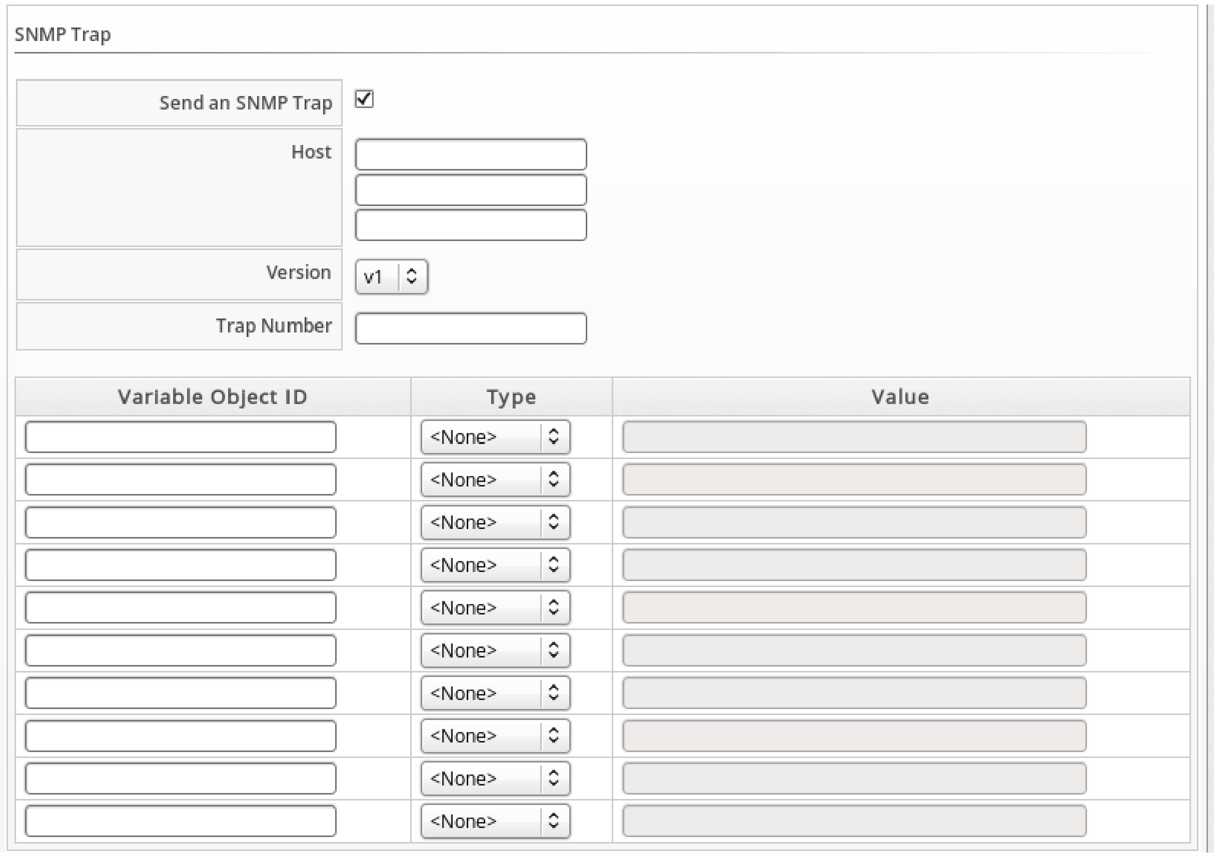
   b. Use **Add a CloudForms Management Engine User** to select a user. The CloudForms Management Engine user must have a valid email address entered under accounts.

   c. Use **Add (enter manually)** to type in the address not registered to a CloudForms Management Engine user. Then, click + (**Add**).

5. If you check **Send an SNMP Trap**, type in the IP for the host to send the trap to, select the version of SNMP that you are using, and type in the Trap Object ID. Type in multiple hosts if you need the trap sent to multiple SNMP hosts.

   - If using SNMP V1, you will be prompted for a Trap Number. Type 1, 2, or 3, based on the appropriate suffix number from table below.
   - If using SNMP V2, you will be prompted for a Trap Object ID. Type info, warning, or critical, based on the table below.
   - Trap Object ID and suffix number

Object ID	Suffix Number Added to PEN	PEN with the Suffix Added
info	1	1.3.6.1.4.1.33482.1
warn, warning	2	1.3.6.1.4.1.33482.2
crit, critical, error	3	1.3.6.1.4.1.33482.3



SNMP Trap

Send an SNMP Trap	☑
Host	
Version	v1
Trap Number	

Variable Object ID	Type	Value
	<None>	
	<None>	
	<None>	
	<None>	
	<None>	
	<None>	
	<None>	
	<None>	
	<None>	
	<None>	

6. To show the alert as an event on the CloudForms Management Engine timeline, check **Show on Timeline**. It shows as part of the Alarm/Status Change/Errors category.

7. To invoke automation, check **Send a Management Event**. Type in the name of the event. This item exists in the **Process/Event Class**.

8. Click **Add**.

7.4. Virtual Machine and Instance Alerts

For virtual machines, you can create alerts based on an event log threshold, an event threshold, normal operating range, and real time performance. You can also create an alert for when CloudForms Management Engine detects that VM hardware has been reconfigured, and when a VM value has been changed. Finally, you can create your own alerts based on a custom expression.

7.4.1. Creating an Event Log Threshold Alert

Use event log thresholds when you want to send a notification when certain items are found in the event logs for a virtual machine. A default analysis profile with event log items is required for this feature. See the *CloudForms Management Engine Insight Guide* for details. In this example, we will check the virtual machines log for an error in the NTP Client.

Procedure 7.3. To Create an Event Log Threshold Alert

1. Navigate to **Control** → **Explorer**.

2. Click on the **Alerts** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Alert**).

3. In the **Info** area:

a. Type in a description for the alert.

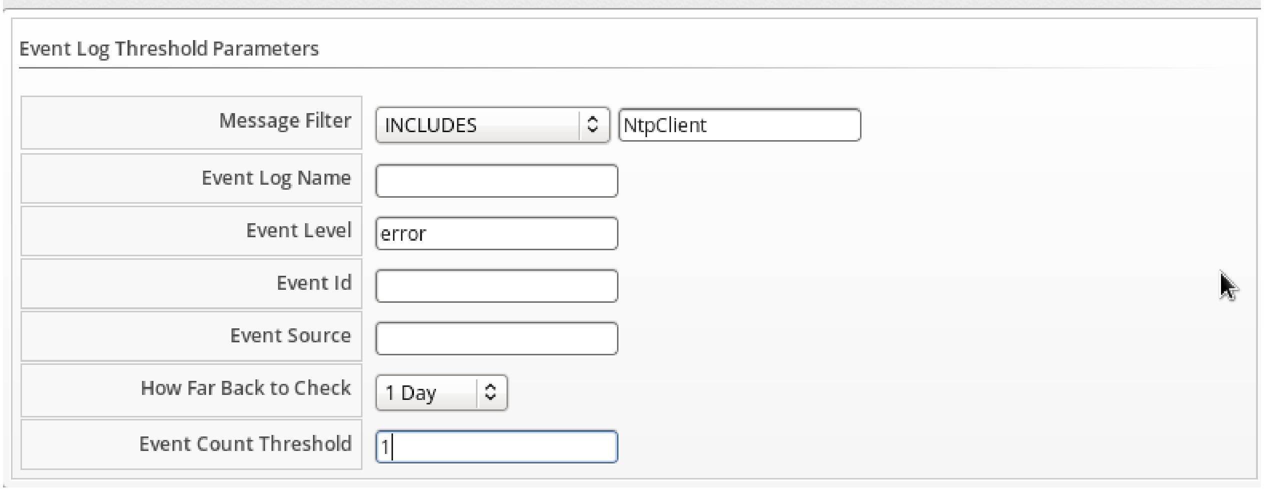
b. Check **Active** when you feel that the alert is ready to be enabled.

c. From **Based On**, select **VM and Instance**.

d. For **What to Evaluate**, select **Event Log Threshold**.

e. In **Notification Frequency**, select how often you want to be notified if the event log threshold is reached.

4. In the **Event Log Threshold Parameters** area, select the parameters for the event log message. You can set a threshold for a filter, level, or message source.



Event Log Threshold Parameters

Message Filter	INCLUDES	NtpClient
Event Log Name		
Event Level	error	
Event Id		
Event Source		
How Far Back to Check	1 Day	
Event Count Threshold	1	

a. Use **Message Filter**, to look for specific text in a message.

b. Use **Event Level** to specify a message level and **Event Id** to filter for an event number. CloudForms Management Engine will report on the specified level and above. Specify an **Event Source** if that is how you want to filter log messages.

c. Set **How Far Back to Check** in time you want to look for this message.

d. If you only need an alert triggered when the log message has occurred a certain number of times, type the number in **Event Count Threshold**.

5. After setting the parameters, select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.

6. Click **Add**.

7.4.2. Creating an Event Threshold Alert

Event threshold alerts are targeted to detect when certain events occur more often than they should for virtual machines. For example, if a virtual machine is powered on too many times in a specific interval.

Procedure 7.4. To Create an Event Threshold Alert

1. Navigate to **Control** → **Explorer**.

2. Click on the **Alerts** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Alert**).

3. In the **Info** area:

   a. Type in a description for the alert.

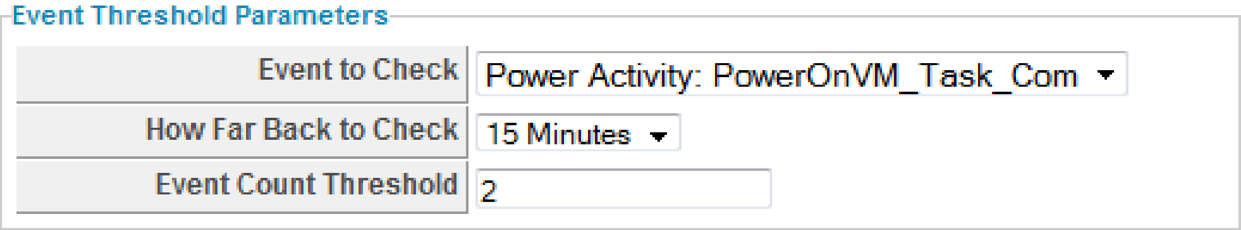
   b. Check **Active** when you feel that the alert is ready to be enabled.

   c. From **Based On**, select **VM and Instance**.

   d. For **What to Evaluate**, select **Event Threshold**.

   e. In **Notification Frequency**, select how often you want to be notified if the event threshold is reached.

4. In the **Event Threshold Parameters** area:



Event Threshold Parameters

Event to Check	Power Activity: PowerOnVM_Task_Com ▾
How Far Back to Check	15 Minutes ▾
Event Count Threshold	2

   a. From **Event to Check**, select **Power Activity: PowerOnVM_Task_Complete**.

   b. From **How Far Back to Check**, select 15 Minutes.

   c. In **Event Count Threshold**, type 2.

5. After setting the parameters, you then select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.

6. Click **Add**.

7.4.3. Creating a Hardware Reconfigured Alert

Use a hardware reconfigure alert to detect changes to the amount of memory or the number of CPUs on a virtual machine.

Procedure 7.5. To Create a Hardware Reconfigure Alert

1. Navigate to **Control** → **Explorer**.

2. Click the **Alerts** accordion, then click ⚙ (**Configuration**), + (**Add a new Alert**).

3. In the **Info** area:

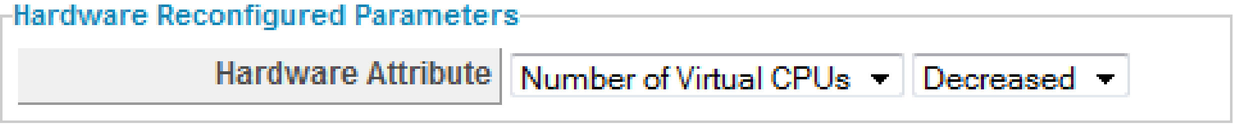
   a. Type in a description for the alert.

   b. From **Based On**, select **VM and Instance**.

   c. From **What to Evaluate**, select **Hardware Reconfigured**.

   d. In **Notification Frequency**, select how often you want to be notified if hardware reconfiguration is detected.

4. From **Hardware Attribute**, select Number of CPUs. From the next dropdown, select **Decreased**.



Hardware Reconfigured Parameters

Hardware Attribute	Number of Virtual CPUs ▾	Decreased ▾

5. After setting the parameters, select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.

6. Click **Add**.

7.4.4. Creating a Normal Operating Range Alert

Normal operating range alerts enables you to be notified when the normal operating range is exceeded, or falls below for a period of time from 1 minute to 2 hours. Capacity and utilization must be enabled for normal operating ranges to be calculated. See the *CloudForms Management Engine Settings and Operations Guide* for instructions.

Procedure 7.6. To Create a Normal Operating Range Alert

1. Navigate to **Control** → **Explorer**.

2. Click the **Alerts** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Alert**).

3. In the **Info** area:

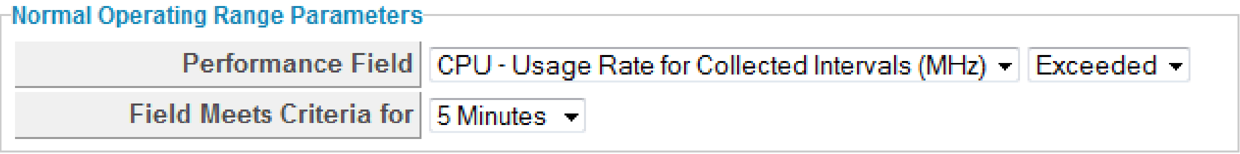
    a. Type in a **Description** for the alert.

    b. From **Based On**, select **VM and Instance**.

    c. For **What to Evaluate**, select **Normal Operating Range**.

    d. In **Notification Frequency**, select how often you want to be notified if the performance threshold is reached.

4. Set the threshold in the **Normal Operating Range Parameters** area.



Normal Operating Range Parameters

Performance Field	CPU - Usage Rate for Collected Intervals (MHz) ▾	Exceeded ▾
Field Meets Criteria for	5 Minutes ▾	

    a. From **Performance Field**, select the field to check and whether you want to be notified if the field is exceeded or fell below.

    b. In **Field Meets Criteria for**, select the amount of time that the threshold requires to be met to trigger the alert.

5. After setting the parameters, you then select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process. See *Creating an Alert*.

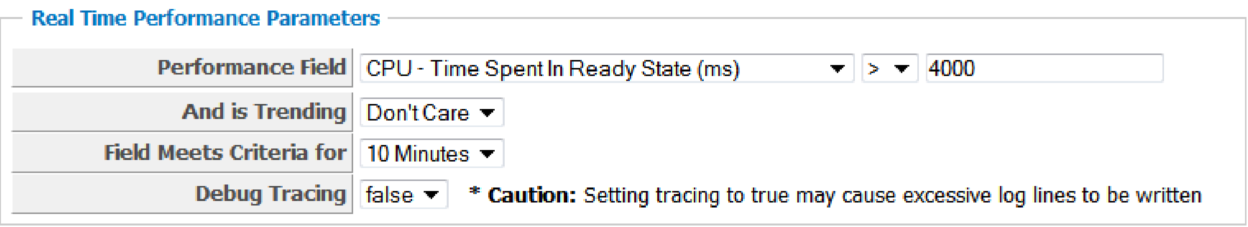
6. Click **Add**.

7.4.5. Creating a Real Time Performance Alert

Real Time Performance alerts enables you to be notified immediately when a performance threshold has been met for a virtual machine, host, or cluster. Capacity and Utilization must be enabled for performance thresholds to be detected. See the *CloudForms Management Engine Settings and Operations Guide* for instructions.

Procedure 7.7. To Create a Real Time Performance Alert

1. Navigate to **Control** → **Explorer**.
2. Click the **Alert** accordion, then click ⚙ (**Configuration**), + (**Add a new Alert**).
3. In the **Info** area:
   a. Type in a **Description** for the alert.
   b. From **Based On**, select **VM and Instance**.
   c. For **What to Evaluate**, select **Real Time Performance**.
   d. In **Notification Frequency**, select how often you want to be notified if the performance threshold is reached.
4. Set the threshold in the **Real Time Performance Parameters** area.



Real Time Performance Parameters

Performance Field	CPU - Time Spent In Ready State (ms)	>	4000
And is Trending	Don't Care		
Field Meets Criteria for	10 Minutes		
Debug Tracing	false	* **Caution:** Setting tracing to true may cause excessive log lines to be written	

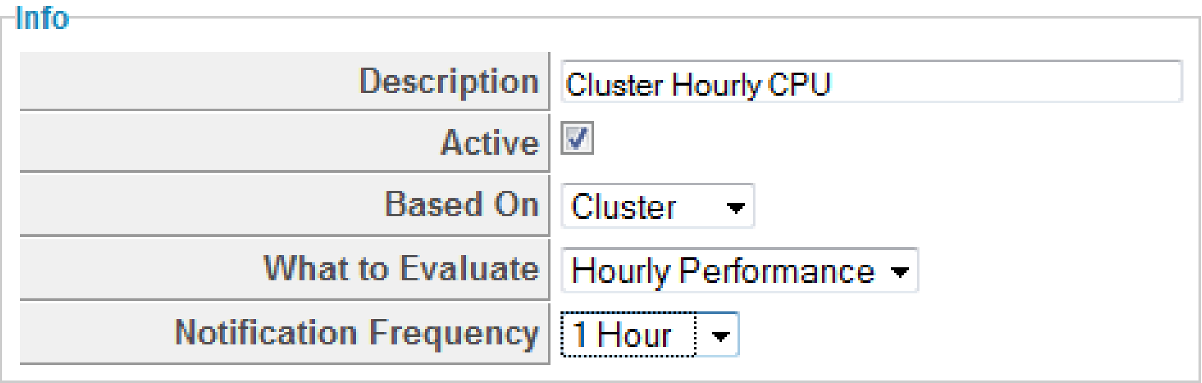
   a. From **Performance Field**, select the field to check and any other parameters required for that field.
   b. In **And is Trending**, select **Don't Care** if it does not matter how the performance metric is trending. Otherwise, choose from the possible trending options.
   c. In **Field Meets Criteria for**, select the amount of time that the threshold requires to be met to trigger the alert.
   d. Set **Debug Tracing** to true only when directed to do so by Red Hat Support. This provides an extremely detailed level of logging and can result in many more log lines being written.
5. After setting the parameters, you then select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.
6. Click **Add**.

7.4.6. Creating an Hourly Performance Alert

Hourly performance alerts enable you to be notified immediately when an hourly performance threshold has been met for a cluster. Capacity and Utilization must be enabled for performance thresholds to be detected. See the *CloudForms Management Engine Settings and Operations Guide* for instructions.

Procedure 7.8. To Create an Hourly Performance Alert

1. Navigate to **Control** → **Explorer**.
2. Click the **Alerts** accordion.
3. Click ⚙ (**`Configuration`**), ✚ (**`Add a new Alert`**).
4. In the **`Info`** area:



Info

Description	Cluster Hourly CPU
Active	☑
Based On	Cluster
What to Evaluate	Hourly Performance
Notification Frequency	1 Hour

   a. Type in a **`Description`** for the alert.

   b. From **`Based On`**, select **Cluster**.

   c. For **`What to Evaluate`**, select **Hourly Performance**.

   d. In **`Notification Frequency`**, select how often you want to be notified if threshold is met.

5. In the **`Hourly Performance Parameters`** area select performance field and the criteria. You can also select options from the **And is Trending** dropdown box and whether the **Debug Tracing** is true or false.
6. After setting the parameters, you then select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.
7. Click **Add**.

7.4.7. Creating a hostd Log Threshold Alert

Use hostd log threshold when you want to send a notification when certain items are found in the event logs for a host. A default analysis profile with event log items is required for this feature. See the *CloudForms Management Engine Insight Guide* for details. In this example, we will check the Hosts log for a failure to validate a virtual machine's IP address.

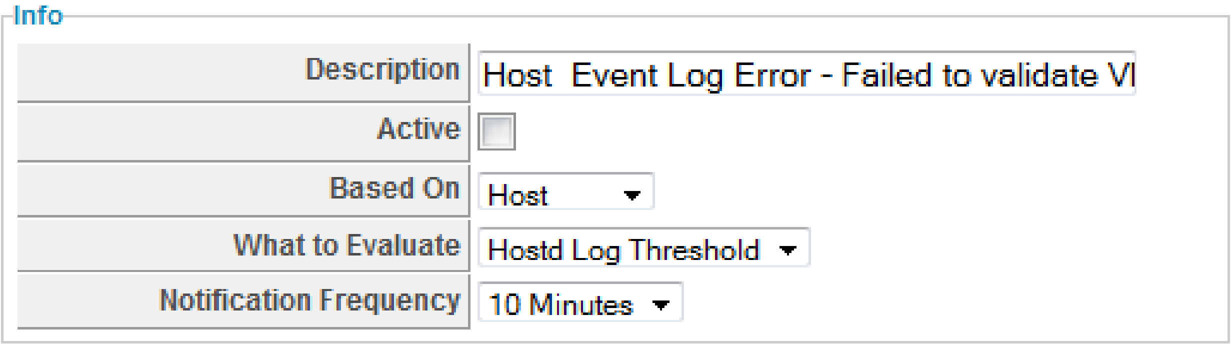
Procedure 7.9. To Create a Hostd Log Threshold Alert

1. Navigate to **Control** → **Explorer**.

2. Click the **Alert** accordion.

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

4. In the **Info** area:



Info

Description	Host Event Log Error - Failed to validate VI
Active	□
Based On	Host
What to Evaluate	Hostd Log Threshold
Notification Frequency	10 Minutes

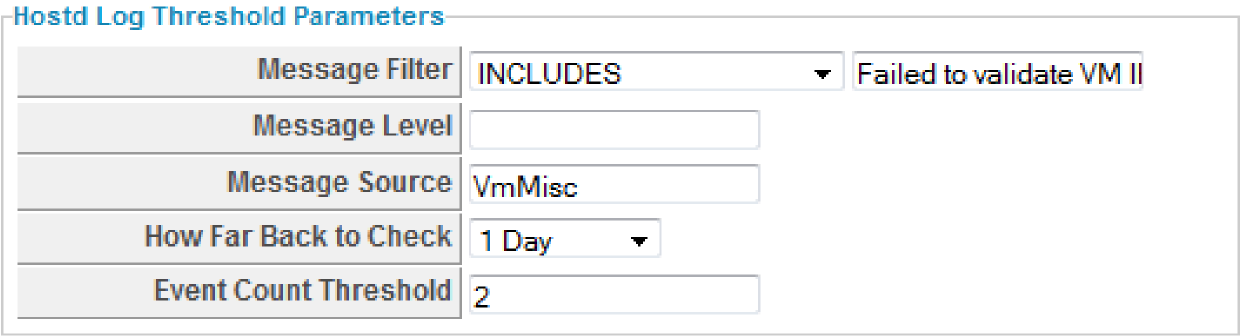
   a. Type in a **Description** for the alert.

   b. From **Based On**, select **Host**.

   c. For **What to Evaluate**, select **Hostd Log Threshold**.

   d. In **Notification Frequency**, select how often you want to be notified if the log item is detected.

5. In the **Hostd Log Threshold Parameters** area, select the parameters for the event log message. You can set a threshold for a filter, level, or message source.



Hostd Log Threshold Parameters

Message Filter	INCLUDES	Failed to validate VM II
Message Level		
Message Source	VmMisc	
How Far Back to Check	1 Day	
Event Count Threshold	2	

   a. Use **Message Filter** to look for specific text in a message. Use **Message Level** to filter based on message level. CloudForms Management Engine reports on the specified level and above. Use **Message Source** to filter log messages based on its source.

   b. Set **How Far Back to Check** in days you want to look for this message.

   c. If you only want an alert triggered when the log message has occurred a certain number of times, type the number in **Event Count Threshold**.

6. After setting the parameters, select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.

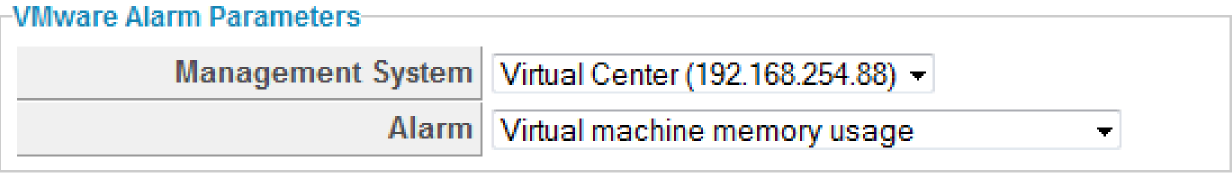
7. Click **Add**.

7.4.8. Creating a VMware Alarm Alert

CloudForms Management Engine can use VMware alarms as a trigger for an alert. This type of alert can be created for a cluster, host, or virtual machine.

Procedure 7.10. To Create a VMware Alarm Alert

1. Navigate to **Control** → **Explorer**.
2. Click the **Alerts** accordion, then click ⚙ (**`Configuration`**), ✚ (**`Add a new Alert`**).
3. In the **Info** area:
    a. Type in a description for the alert.
    b. From **`Based On`**, select **Cluster**, **Host**, or **VM**.
    c. For **`What to Evaluate`**, select **VMware Alarm**.
    d. In **`Notification Frequency`**, select how often you want to be notified if the log item is detected.
4. In the **`VMware Alarm Parameters`** area select the provider and alarm.



VMware Alarm Parameters

Management System	Virtual Center (192.168.254.88)
Alarm	Virtual machine memory usage

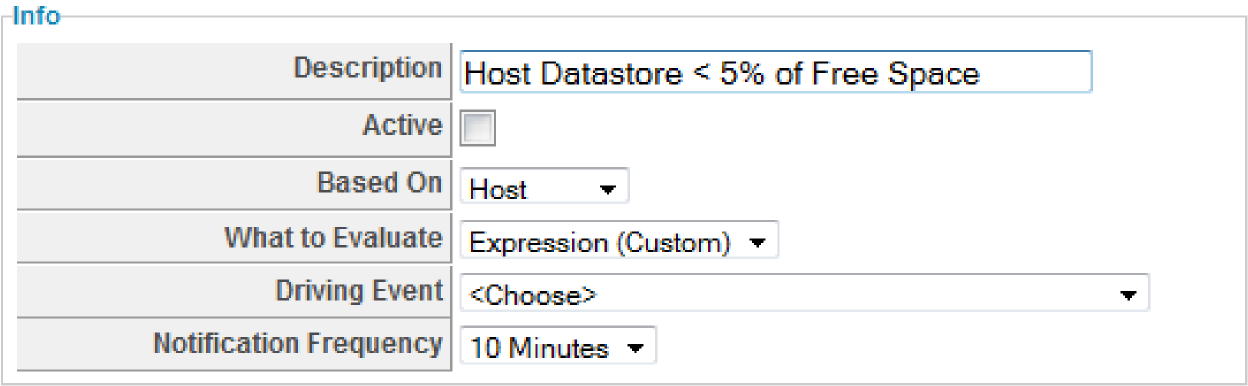
5. After setting the parameters, you then select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.
6. Click **Add**.

7.4.9. Creating an Expression Alert

Expression alerts enables you to create a notification based on any possible criteria for clusters, datastores, hosts, and virtual machines. In the example below, we look for a host whose datastore has less than 5% free space.

Procedure 7.11. To Create an Expression Alert

1. Navigate to **Control** → **Explorer**.
2. Click on the **Alerts** accordion, then click ⚙ (**`Configuration`**), ✚ (**`Add a new Alert`**).
3. In the **Info** area:



Info

Description	Host Datastore < 5% of Free Space
Active	□
Based On	Host
What to Evaluate	Expression (Custom)
Driving Event	<Choose>
Notification Frequency	10 Minutes

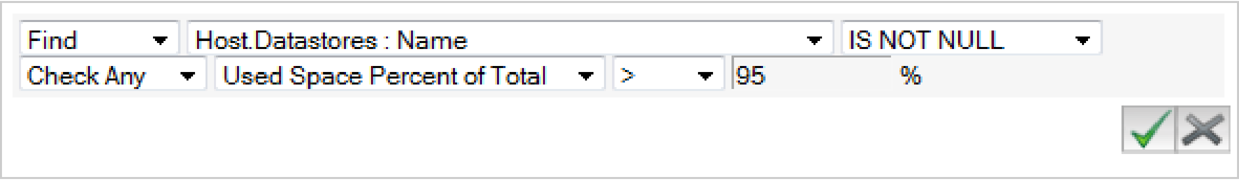
a. Type in a description for the alert.

b. From **Based On**, select **Host**.

c. For **What to Evaluate**, select **Expression (Custom)**.

d. In **Notification Frequency**, select how often you want to be notified if the expression is evaluated to true.

4. Use the expression editor to create your expression. This is the same expression editor used to create Conditions. For details on how to use the expression editor, see Creating a Condition.



Find	Host.Datastores : Name	IS NOT NULL		
Check Any	Used Space Percent of Total	>	95	%

5. Click ✓ (**Commit expression element changes**) to accept the expression.

6. After setting the parameters, you then select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.

7. Click **Add**.

7.5. CloudForms Management Engine Operational Alerts

CloudForms Management Engine provides the ability to notify you when certain operational events occur. These can be configured as alerts from the Control page in the CloudForms Management Engine Console. Once the Alert and the Alert Profiles are created, you can assign them to CloudForms Management Engine Servers in the current Region.

7.5.1. Create an Operational Alert

Procedure 7.12. To Create an Operational Alert

1. Navigate to **Control** → **Explorer**.

2. Click on the **Alerts** accordion, then click ⚙ (**Configuration**), + (**Add a new Alert**).

3. In the **Info** area:

   a. Type in a description for the alert.

   b. Check **Active** when you feel that the alert is ready to be enabled.

   c. From **Based On**, select **Server**.

   d. Select the appropriate driving event.

   e. In **Notification Frequency**, select how often you want to be notified if the event log threshold is reached.

4. After setting the parameters, select what you want the alert to do. You can send an email, create an SNMP Trap, let the alert show on the timeline, or send a management event to start an automation process.

5. Click **Add**.

7.5.2. Operational Alert Types

Table 7.1. Operational Alerts

Driving Event	Explanation (Thresholds, Description)	Proposed Action if Alert is Raised
EVM Server Start	Alert is raised when an EVM Server starts.	
EVM Server Stop	Alert is raised when an EVM Server stops.	
EVM Server Not Responding	Alert is raised when one EVM server detects that another EVM Server has not responded in (2 minutes).	This is a sign of a problem that should be investigated. Check logs.
EVM Server Exceeded Memory Limit	Alert is raised when an EVM server has exceeded its system memory limit and begins killing workers. Default is 80%. Threshold configured in Advanced Settings. server: :worker_monitor: :kill_algorithm: :name: :used_swap_percent_gt_value :value: 80	This may be caused by the following issues: » The server is running with too few resources. » The server is enabled with too many roles or number of workers. » The server picked up all the roles because another server has failed. » A runaway process has taken up most of the memory.

Driving Event	Explanation (Thresholds, Description)	Proposed Action if Alert is Raised
EVM Server is Master	When one EVM Server takes over as a master server.	Typically, this should only occur when first starting a set of servers, perhaps following expected outages. If a server picks up as master in other situations, the old master had an issue that needs to be researched (such as server not responding in time).
EVM Server High System Disk Usage	The EVM Servers system disk is 80% full. This check is run as part of a system schedule. Threshold configured in Advanced Settings. server: events: :disk_usage_gt_percent: 80	Something is filling the disk such as temp files used by the operating system such as, yum updates and normal /tmp files, or EVM temp files in /var/lib/data/miqtemp/.
EVM Server High App Disk Usage	The EVM Servers app disk is 80% full. This check is run as part of a system schedule. Threshold configured in Advanced Settings. server: events: :disk_usage_gt_percent: 80	Possibly EVM temp files are being left around.
EVM Server High Log Disk Usage	The EVM Servers log disk is 80% full. This check is run as part of a system schedule. Threshold configured in Advanced Settings. server: events: :disk_usage_gt_percent: 80	Logs are getting too big or are not being log rotated properly every day. Check most recent logs.

Driving Event	Explanation (Thresholds, Description)	Proposed Action if Alert is Raised
EVM Server High DB Disk Usage	The EVM Servers db disk is 80% full. This check is run as part of a system schedule. Applies if using PostgreSQL as the VDMB. Threshold configured in Advanced Settings. server: events: :disk_usage_gt_percent: 80	Database or database logging is getting too large. May need FULL vacuuming of PostgreSQL database.
EVM Worker Started	Alert is raised when a worker is about to start.	
EVM Worker Stopped	Alert is raised when a worker is requested to stop.	
EVM Worker Killed	Alert is raised when a non-responsive worker does not restart on its own and is killed.	
EVM Worker Not Responding	Alert is raised when a worker has not responded for 2 minutes (:heartbeat_timeout) or has not started within 10 minutes (:starting_timeout).	
EVM Worker Exceeded Memory Limit	Alert is raised when a worker exceeds the memory threshold. The default is 150 MB, but some workers have their own value in the :memory_threshold section for that specific worker.	
EVM Worker Exceeded Uptime Limit	Alert is raised when a worker has been running longer than the :restart_interval. (Most workers are set to never restart using the 0.hours setting.) The EMS Refresh SmartProxy workers are set to restart every 2 hours.	
EVM Worker Exit File	Alert is raised when the scheduler worker exits due to a pending large ntp time change.	

7.6. Editing an Alert

After creating an alert, you can edit the threshold, expression, or the notification type.

Procedure 7.13. To Edit an Alert

1. Navigate to **Control** → **Explorer**

2. Click on the **Alerts** accordion, then click on the alert that you need to edit.

3. Click ⚙ **(Configuration)**, ✎ **(Edit this Alert)**.

4. Make the required changes.

5. Click **Save**.

7.7. Copying an Alert

You can copy an existing alert to create a new alert that is similar to the existing one, then change the values associated with it.

Procedure 7.14. To Copy an Alert

1. Navigate to **Control** → **Explorer**.

2. Click on the **Alert** accordion, then click on the alert that you want to copy.

3. Click ⚙ (**Configuration**), ⧉ (**Copy this Alert**). Click **OK** to confirm.

4. Make the required changes.

5. Click **Add**.

7.8. Deleting an Alert

When an alert is no longer needed, you can remove it from your VMDB

Procedure 7.15. To Delete an Alert

1. Navigate to **Control** → **Explorer**.

2. Click on the **Alerts** accordion, then click on the alert that you want to delete.

3. Click ⚙ (**Configuration**), 🗑 (**Delete this Alert**).

4. Click **OK** to confirm.

7.9. Evaluating an Alert

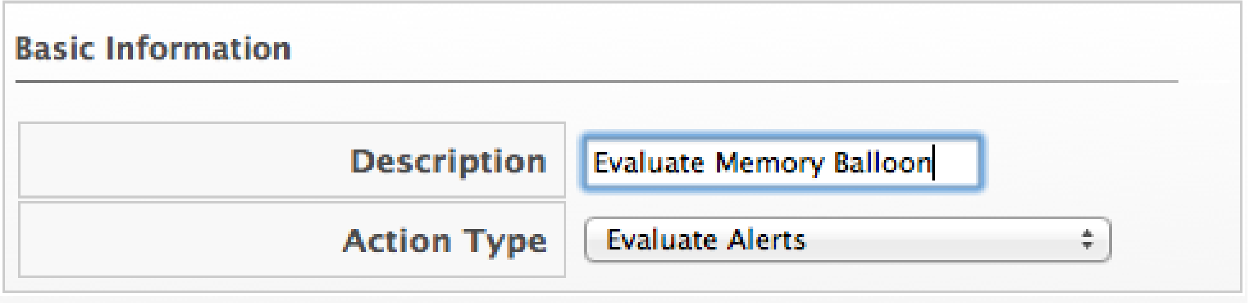
An alert can either stand on its own or be assigned to a policy. To assign it for use in a policy, use the evaluate alert action.

Procedure 7.16. To Evaluate an Alert

1. Navigate to **Control** → **Explorer**

2. Click on the **Actions** accordion, then click ⚙ (**Configuration**), ✚ (**Add a new Action**).

3. Type in a **Description** for the action.



Basic Information

Description	Evaluate Memory Balloon
Action Type	Evaluate Alerts

4. Select **Evaluate Alerts** from **Action Type**.

5. Select the alerts to be evaluated and click ▶ (Move selected Alerts into this Action). Use **Ctrl** to move multiple alerts.

6. Click **Add**.

Chapter 8. Alert Profiles

8.1. Creating Alert Profiles

Alert profiles enable you to create groups of standard alerts. An alert profile can have as many alerts assigned as you need, and can be assigned to clusters, datastores, hosts, and virtual machines.

Procedure 8.1. To Create an Alert Profile

1. Navigate to **Control** → **Explorer**.
2. Click on the **Alert Profiles** accordion, then click on the type of profile that you want to create.
3. Click ⚙ (**Configuration**), ✚ (**Add a new Profile**).
4. In the **Basic Information** box, type in a unique **Description** for the alert profile.
5. Select the desired alerts from the **Available Datastore Alerts** area. Use the **Ctrl** key to select multiple alerts.
6. Click ▶ to add the Alerts.
7. Type in any additional description in the **Notes** area.
8. Click **Add**.

8.2. Editing an Alert Profile

You can edit an alert profile as your enterprise's need change.

Procedure 8.2. To Edit an Alert Profile

1. Navigate to **Control** → **Explorer**.
2. Click on the **Alert Profiles** accordion, then click the alert profile you want to edit.
3. Click ⚙ (**Configuration**), ✎ (**Edit this Alert Profile**).
4. Make the required changes.
5. Click **Save**.

8.3. Deleting an Alert Profile

Remove alert profiles that you no longer need. This does not remove the alerts associated with the alert profile.

Procedure 8.3. To Delete an Alert Profile

1. Navigate to **Control** → **Explorer**.
2. Click on the **Alert Profiles** accordion, then click the alert profile you want to remove.

3. Click ⚙ (**Configuration**), 🗑 (**Delete this Alert Profile**).

4. Click **OK** to confirm.

8.4. Assigning an Alert Profile

After an alert profile is created and verified, you can assign it directly to a resource.

Procedure 8.4. To Assign an Alert Profile

1. Navigate to **Control** → **Explorer**.

2. Click on the **Alert Profiles** accordion, then click on the alert profile that you want to assign.

3. Click ⚙ (**Configuration**), 📋 (**Edit Assignments for this Alert Profile**).

4. The options presented change based on if the alert is for a cluster, datastore, CloudForms Management Engine server, host, or virtual machine and instance. You can assign to the enterprise, to specific hosts, cluster, resource pools, and providers, or based on assign tags. For a CloudForms Management Engine server alert profile, you can only assign to CloudForms Management Engine servers in the current Region.

5. Click **Save**.

Chapter 9. Importing and Exporting

9.1. Importing and Exporting Policies, Policy Profiles, and Alerts

If you have multiple VMDBs, you can export policies, policy profiles, or alerts from one to another. You can export and import for use with other CloudForms Management Engine infrastructures.

Procedure 9.1. To Import a Policy, Policy Profile, or an Alert

1. Copy the file to import to a location that is accessible to your CloudForms Management Engine Console.

2. Navigate to **Control** → **Import/Export**.

3. Click **Browse** to navigate to the location of the file.

4. Select the file, and then click **Open** from the file selection box.

5. Click **Upload**.

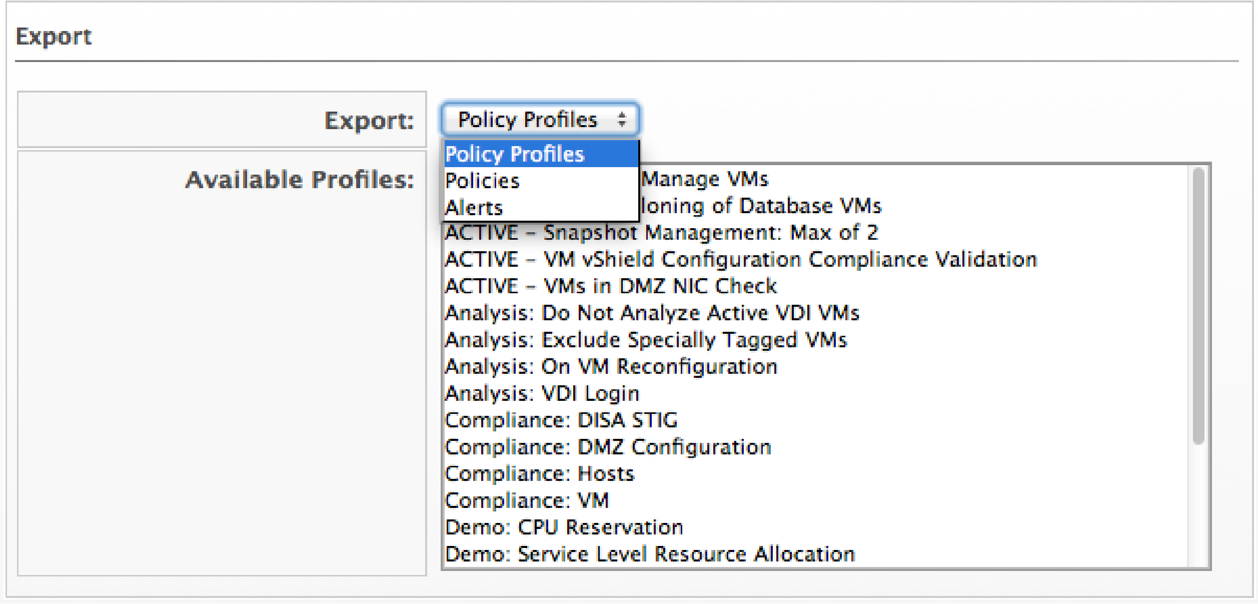
6. Verify that these are the policies or policy profiles that you want to import.

7. Click **Commit**.

9.2. Exporting a Policy, Policy Profile, or an Alert

1. Navigate to **Control** → **Import/Export**.

2. From the **Export dropdown**, select policy profiles, policies, or alerts, depending on what you want to export.


Export
Export:
Policy Profiles
Policy Profiles
Policies
Alerts
Available Profiles:
Manage VMs
loning of Database VMs
ACTIVE – Snapshot Management: Max of 2
ACTIVE – VM vShield Configuration Compliance Validation
ACTIVE – VMs in DMZ NIC Check
Analysis: Do Not Analyze Active VDI VMs
Analysis: Exclude Specially Tagged VMs
Analysis: On VM Reconfiguration
Analysis: VDI Login
Compliance: DISA STIG
Compliance: DMZ Configuration
Compliance: Hosts
Compliance: VM
Demo: CPU Reservation
Demo: Service Level Resource Allocation

3. From the **Available Profiles** or **Available Policies** or **Available Alerts** list, select the items to export. Use the **Ctrl** key to select multiple items to export into one file.

4. Click **Export**.

5. Follow the prompts in your browser to save the file.

Chapter 10. Resource Control

10.1. Accessing Virtual Machines and Hosts

This chapter details the CloudForms Management Engine Control feature set. These buttons enable you to control the power state of virtual machines; view timelines of the policy events for a virtual machine, host, provider, or cluster; and enable viewing through a web console.

For a general overview of the virtual machine, infrastructure component, and storage location buttons see the *CloudForms Management Engine Insight Guide*.

10.1.1. Controlling Virtual Machines

You can start, stop, and suspend a virtual machine through the CloudForms Management Engine console. To do this, the following requirements must be met:

- The virtual machine must be discovered.
- The virtual machine must be registered to a host and have a SmartProxy associated with it.
- The virtual machine cannot be in **Infrastructure** → **Repositories**.

10.1.1.1. Controlling the Power State of Virtual Machines

Start, stop, and suspend any number of virtual machines through the CloudForms Management Engine console using the following procedure.

Procedure 10.1. To Control the Power State of Virtual Machines

1. Navigate to **Infrastructure** → **Virtual Machines**.
2. Check the virtual machines that you want to change the power state for.
3. Click ⏻ (**`Power Operations`**). Note that the only operations that will be available are the ones that apply to the virtual machines' current power state.
4. Click the button for the power operation you want.
   a. Click ⏻ (**`Power On`**) to start the selected virtual machines.
   b. Click ⏻ (**`Power Off`**) to stop the selected virtual machines.
   c. Click ⏸ (**`Suspend`**) to suspend the selected virtual machines.
   d. Click 🔄 (**`Reset`**) to stop the selected virtual machines.
   e. Click 🟥 (**`Shutdown Guest`**) to stop the guest operating system.
   f. Click 🔄 (**`Restart Guest`**) to restart the guest operating system.
5. Click **`OK`** to confirm.

10.1.2. Retiring Virtual Machines

CloudForms Management Engine Control allows you to retire a virtual machine on a specific date or immediately. When a virtual machine is retired, it cannot start. There are three built-in policies involved with virtual machine retirement.

- When the virtual machine reaches the retire date, it is stopped if it is running.
- When a retired virtual machine is requested to start through CloudForms Management Engine, the virtual machine cannot start.
- When a provider starts a retired virtual machine outside of CloudForms Management Engine, the virtual machine is stopped.

10.1.2.1. Setting a Retirement Date for a Virtual Machine

CloudForms Management Engine enables you to retire a virtual machine on a specific date.

Procedure 10.2. To Set a Retirement Date for a Virtual Machine

1. From **Infrastructure** → **Virtual Machines**, click on the virtual machine that you want to set a retirement date for.
2. Click ♻ (**Lifecycle**), ⏱ (**Set Retirement Dates**).
3. In the **Retirement Date** field, type in the desired retirement date, or you can select one from the calendar control.
4. Click **Save**.

10.1.2.2. Removing a Retirement Date for a Virtual Machine

CloudForms Management Engine enables you to remove a retirement date for virtual machines.

Procedure 10.3. To Remove a Retirement Date for a Virtual Machine

1. From **Infrastructure** → **Virtual Machines**, click on the virtual machine that you want to remove the retirement date from.
2. Click ♻ (**Lifecycle**), ⏱ (**Set Retirement Dates**).
3. Click ✗ (**Remove retirement date**).

10.1.2.3. Immediately Retiring a Virtual Machine

CloudForms Management Engine enables you to retire a virtual machine immediately.

Procedure 10.4. To Immediately Retire a Virtual Machine

1. From **Infrastructure** → **Virtual Machines**, click on the virtual machine that you need to remove the retirement date from.
2. Click ♻ (**Lifecycle**), ⏱ (**Retire Selected Items**).

Result:

The virtual machine is immediately stopped and cannot restart.

10.1.3. Creating and Deleting Snapshots

Use CloudForms Management Engine Control to create, remove, and revert snapshots for your virtual machines.

10.1.3.1. Creating a Snapshot

Create a new snapshot before making changes to a virtual machine.

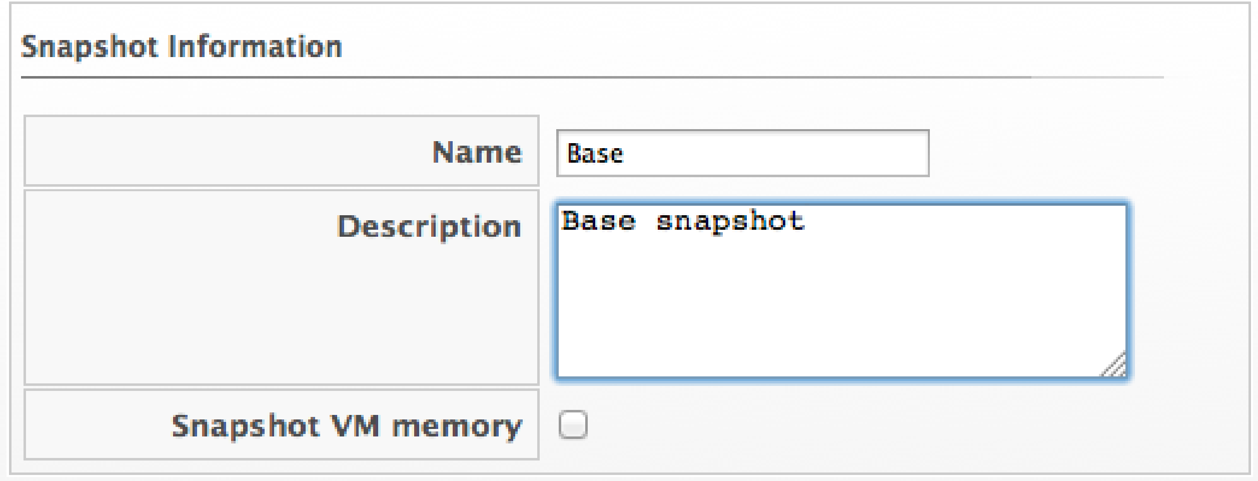
Procedure 10.5. To Create a Snapshot

1. From **Infrastructure** → **Virtual Machines**, click on the virtual machine that you want to create a snapshot for.

2. From the **Properties** area, click **Snapshots**.

3. Click ✚ (**Create a new snapshot of this VM**).

4. Type in a **Name** and **Description**. Check **Snapshot VM memory** if you want this option.



Snapshot Information

Name	Base
Description	Base snapshot
Snapshot VM memory	☐

5. Click **Create**.

10.1.3.2. Deleting a Snapshot

CloudForms Management Engine enables you to delete snapshots when you no longer need them.

Procedure 10.6. To Delete a Snapshot

1. From **Infrastructure** → **Virtual Machines**, click on the virtual machine that you want to remove the snapshot from.

2. From the **Properties** area, click **Snapshots**.

3. Select the snapshot that you want to remove.

4. Click 🗑 (**Delete Snapshots**), and then 🗑 (**Delete Selected Snapshot**).

5. Click **OK** to confirm.

10.1.3.3. Deleting All Snapshots

CloudForms Management Engine enables you to delete snapshots when you no longer need them.

Procedure 10.7. To Delete All Snapshots

1. From **Infrastructure** → **Virtual Machines**, click on the virtual machine that you want to remove all snapshots from.
2. From the **Properties** area, click snapshots.
3. Click 🗑 (**Delete Snapshots**), and then 🗑 (**Delete All Existing Snapshots**).
4. Click **OK** to confirm.

> **Note**
>
> The snapshot deletion process can be followed under **Settings & Operations Tasks** → **My Other UI Tasks**. If new snapshots have made the virtual machine unusable, you can revert it from the CloudForms Management Engine console.

10.1.3.4. Reverting to a Previous Snapshot

Procedure 10.8. To Revert to a Previous Snapshot

1. From **Infrastructure** → **Virtual Machines**, click on the virtual machine that you want to revert to a previous snapshot.
2. From the **Properties** area, click snapshots.
3. From the list of available snapshots, click the one you want to go back to.
4. Click ⏪ (**Revert to selected snapshot**).
5. Click **OK** to confirm.

10.2. Accessing Cloud Instances

The *CloudForms Management Engine Insight Guide* describes the buttons for instances. This guide describes the additional buttons available with the CloudForms Management Engine Control feature set. These buttons allow you to control the power state of instances.

10.2.1. Controlling Instances

You can start and stop an instance through the CloudForms Management Engine Console. To do this, the following requirements must be met:

- The instance must be discovered.
- The instance must be registered to a host and have a SmartProxy associated with it.

10.2.1.1. Terminating the Power State of Instances

Stop any number of instances through the CloudForms Management Engine console using the following procedure.

Procedure 10.9. To Terminate the Power State of Instances

1. Navigate to **Clouds** → **Instances**.
2. Check the instances that you want to terminate.
3. Click ⏻ (**`Power Operations`**). Note that the only operations that will be available are the ones that apply to the instances' current power state.
4. Click ⏻ (**`Terminate`**) to stop the selected instances.
5. Click **`OK`** to confirm.

10.2.2. Retiring Instances

CloudForms Management Engine Control allows you to retire an instance on a specific date or immediately. When an instance is retired, it will not be allowed to start. There are three built-in policies involved with instance retirement.

- When the instance reaches the retire date, it will be stopped if it is running.
- When a retired instance is requested to start through CloudForms Management Engine, the instance will not be allowed to start.
- When a provider starts a retired instance outside of CloudForms Management Engine, the instance will be stopped.

10.2.2.1. Setting a Retirement Date for an Instance

CloudForms Management Engine allows you to retire an instance on a specific date.

Procedure 10.10. To Set a Retirement Date for an Instance

1. From **Clouds** → **Instances**, click on the instance that you want to set a retirement date for.
2. Click ♻ (**`Lifecycle`**), then click ⏱ (**`Set Retirement Dates`**).
3. Either type in a date in the **`Retirement Date`** field or select one from the calendar control.
4. Click **`Save`**.

10.2.2.2. Removing a Retirement Date for an Instance

CloudForms Management Engine allows you to remove a retirement date for instances.

Procedure 10.11. To Remove a Retirement Date for an Instance

1. From **Clouds** → **Instances**, click on the instance that you want to remove the retirement date from.
2. Click ♻ (**`Lifecycle`**), and then click ⏱ (**`Set Retirement Dates`**).

3. Click ❌ (**`Remove retirement date`**).

10.2.2.3. Immediately Retiring an Instance

CloudForms Management Engine allows you to retire an instance immediately.

Procedure 10.12. To Immediately Retire an Instance

1. From **Clouds** → **Instances**, click on the instance that you want to remove the retirement date from.
2. Click ♻ (**`Lifecycle`**).
3. Click ⏱ (**`Retire Selected Items`**).

Result:

The instance is immediately stopped and cannot restart.

Regular Expressions

In CloudForms Management Engine, regular expressions can be used to search the contents of a file for a specific string for use in a condition. Below are listed the items most commonly used with CloudForms Management Engine to search strings. These are a small subset of all the items available to use in regular expressions. If you are unfamiliar with regular expressions, there are many resources available on the Internet, including www.regular-expressions.info. Note that if you want to search a file, you must collect it as part of a host analysis profile.

Table A.1. Regular Expressions

<table>
<tr><td>Anchors</td><td></td></tr>
<tr><td>^</td><td>start of string</td></tr>
<tr><td>$</td><td>end of string</td></tr>
<tr><td>Character Classes</td><td></td></tr>
<tr><td>\s</td><td>white space including spaces, tabs, and line breaks</td></tr>
<tr><td>\S</td><td>not white space</td></tr>
<tr><td>\d</td><td>digit, same as [0-9]</td></tr>
<tr><td>\D</td><td>not digit</td></tr>
<tr><td>\w</td><td>word</td></tr>
<tr><td>\W</td><td>not word</td></tr>
<tr><td>Quantifiers</td><td></td></tr>
<tr><td>*</td><td>0 or more of preceding characters</td></tr>
<tr><td>+</td><td>1 or more of preceding characters</td></tr>
<tr><td>?</td><td>0 or 1 of preceding character</td></tr>
<tr><td>Escape Character</td><td></td></tr>
<tr><td>\</td><td>put before a metacharacter to search for that actual character</td></tr>
<tr><td>Metacharacters</td><td></td></tr>
<tr><td>^ [. $ { * (\ +) | ? < ></td><td>must be used with the Escape Character if you are searching specifically for it</td></tr>
<tr><td>Special characters</td><td></td></tr>
<tr><td>\n</td><td>new line</td></tr>
<tr><td>\t</td><td>tab</td></tr>
<tr><td>Groups and Ranges</td><td></td></tr>
<tr><td>.</td><td>any character except new line (\n)</td></tr>
<tr><td>(a|b)</td><td>a or b</td></tr>
<tr><td>()</td><td>group</td></tr>
<tr><td>[abc]</td><td>a or b or c</td></tr>
<tr><td>[^abc]</td><td>not a or b or c</td></tr>
<tr><td>[a-q]</td><td>letter between a and q</td></tr>
<tr><td>[A-Q]</td><td>upper case letter between A and Q</td></tr>
<tr><td>[0-7]</td><td>digit between 0 and 7</td></tr>
<tr><td>Pattern modifiers</td><td></td></tr>
<tr><td>i</td><td>case insensitive</td></tr>
<tr><td>Other helpers</td><td></td></tr>
<tr><td>.*</td><td>swallows text between 2 words</td></tr>
<tr><td>\s+</td><td>guarantees minimum of 1 whitespace between 2 words</td></tr>
</table>

\s*	guarantees 0 or more whitespace between 2 words
^\s*	beginning of line with zero or more whitespace
\s+.*	swallows all text and white space between 2 words
\d+	guarantees minimum of 1 number between 2 words
<\w>	identical to <[a-zA-Z0-(_]>

Table A.2. Examples

Description	Regular Expression
([A-Za-z0-9]+)	Letters, numbers, hyphens
Find the line beginning with sshd. Then, using a colon : as delimiter, check that the value four ":" over is equal to 99999	^sshd:[^:]*:[^:]*:[^:]*:99999:
Verify that PASS_MAX_DAYS exists starting in position 1 and a value after it is <= 90	^\s*PASS_MAX_DAYS\s+([0-9]|[1-8][0-9]|90)
Verify that ROOTPW (in any case) exists on an uncommented line	/^[^#]*ROOTPW/i
Verify that line in file starts with size and the value after is <= 4096k	^\s*size\s+(409[0-6]|40[0-8][0-9]|[123][09]{3}|\d{1,3})k
Find line with string restrict 127.0.0.1 that starts in position 1 to ensure it is not commented out	^\s*restrict\s+127\.0\.0\.1
Find an uncommented line that contains "/home". There will be additional text before the desired string	^[^#]*\/home

Revision History

Revision 0.0.0-2	Tue Sep 2 2014	CloudForms Docs Team

Initial book creation.