Red Hat CloudForms 4.5

Policies and Profiles Guide

Policy-based enforcement, compliance, events, and policy profiles for Red Hat CloudForms

Last Updated: 2018-04-27

Red Hat CloudForms 4.5 Policies and Profiles Guide

Policy-based enforcement, compliance, events, and policy profiles for Red Hat CloudForms

Red Hat CloudForms Documentation Team
cloudforms-docs@redhat.com

Legal Notice

Abstract

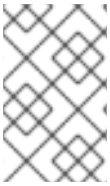
This guide provides instructions for policy-based actions in a Red Hat CloudForms environment, including system controls, enforcement, compliance, and events. Information and procedures in this book are relevant to Red Hat CloudForms administrators. If you have a suggestion for improving this guide or have found an error, please submit a Bugzilla report at http://bugzilla.redhat.com against Red Hat CloudForms Management Engine for the Documentation component. Please provide specific details, such as the section number, guide name, and CloudForms version so we can easily locate the content.

Table of Contents

CHAPTER 1. 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.



NOTE

Red Hat CloudForms also provides a built-in OpenSCAP policy profile. You can assign this profile to apply baseline security and compliance for container images. See Section A.2, “OpenSCAP Integration” for more information.

1.1. 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.

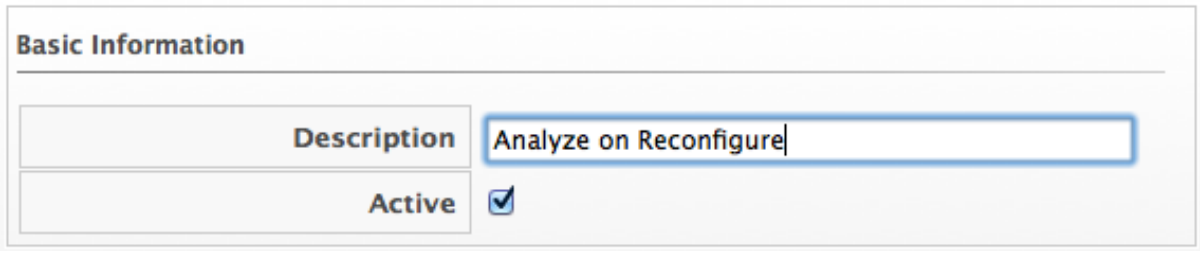
1.1.1. Creating Control Policies

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.

1. Navigate to **Control** → **Explorer**.
2. Click the **Policies** accordion, and select **Control Policies**.
3. Select either **Host Control Policies** or **VM Control Policies** or **Replicator Control Policies** or **Pod Control Policies** or **Container Node Control Policies** or **Container Image Control Policies**.
4. Click  **(Configuration)**,  **(Add a New Host / VM / Replicator / Pod / Node / Image Control Policy)**.

5. Type in a **Description**.

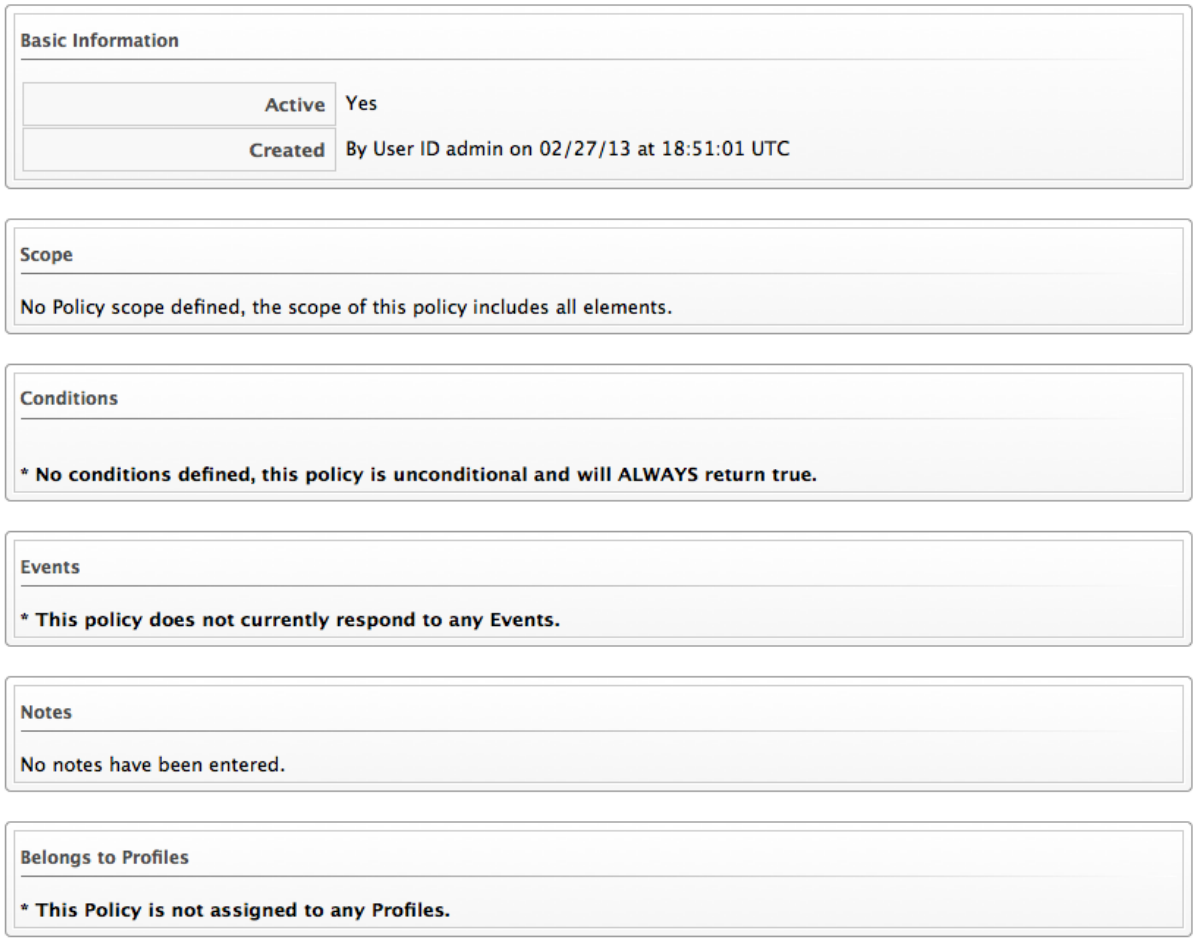


6. Uncheck **Active** if you do not want this policy processed even when assigned to a resource.

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.



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

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

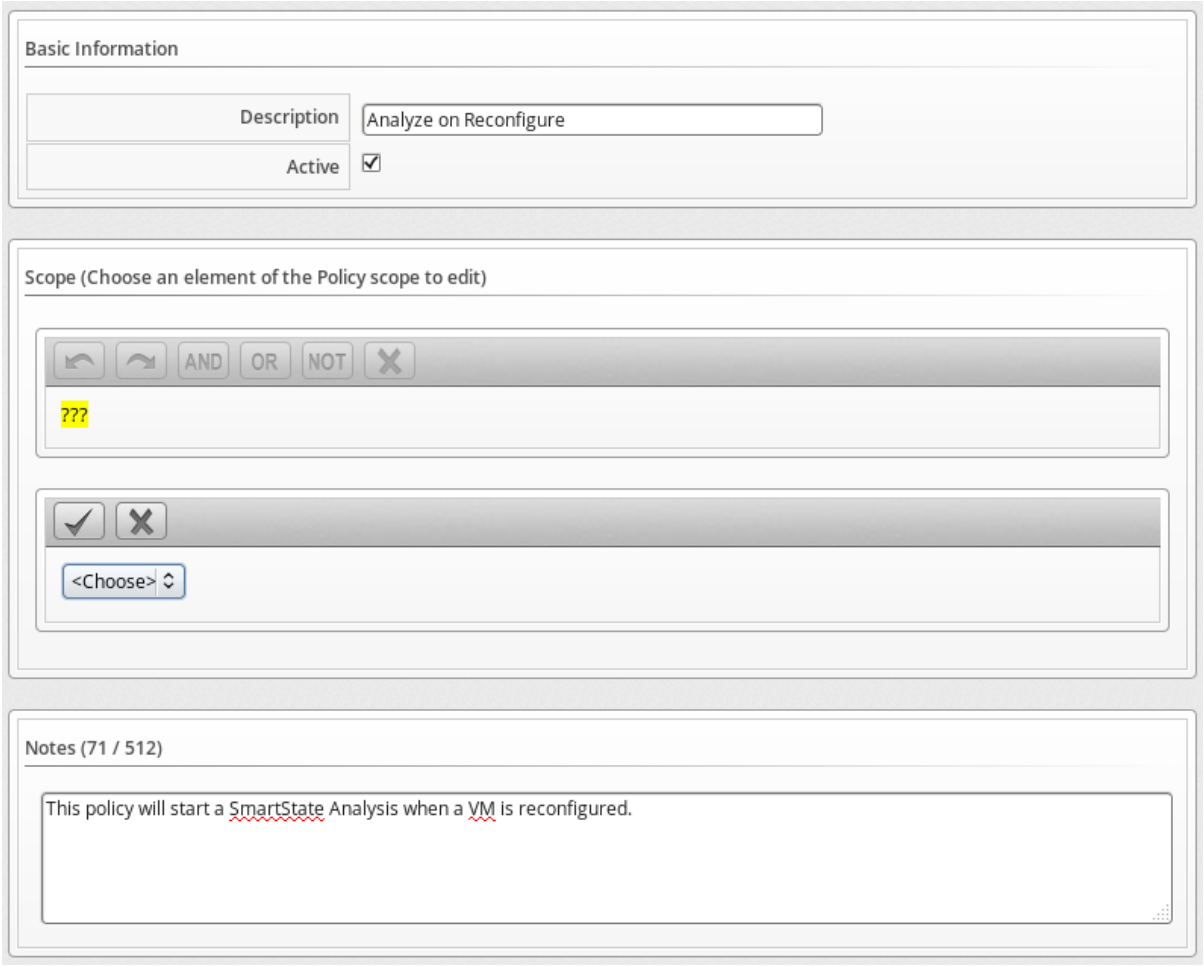
As your enterprise's needs change, you can change the name of a policy or its scope. If the items being evaluated are out of scope, policy processing stops and no actions run.

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

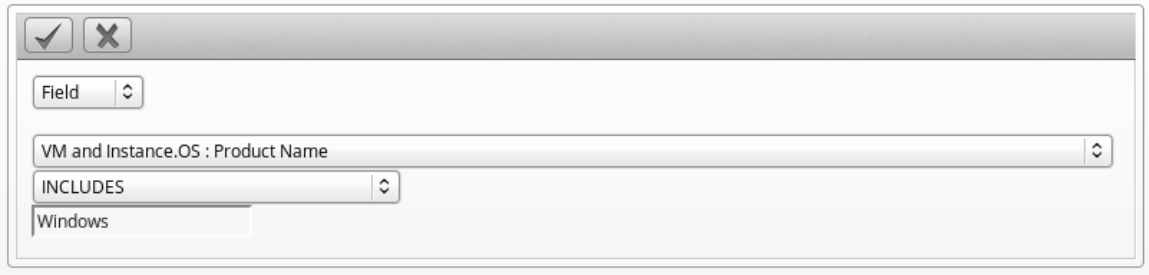
2. Click the **Policies** accordion, and select the policy to edit.

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. Configuring a **Scope** is optional for a policy.

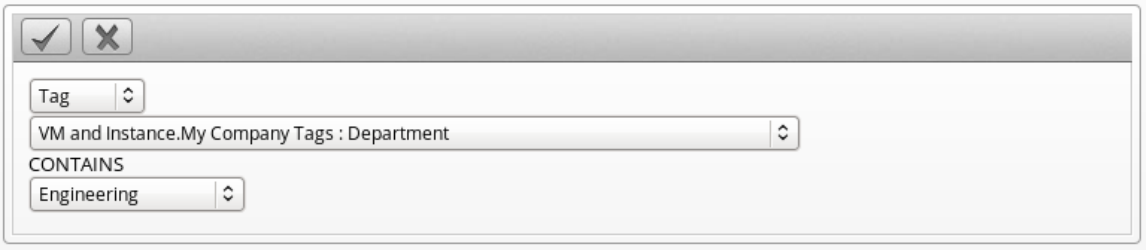


- Click **Field** to create criteria based on field values.



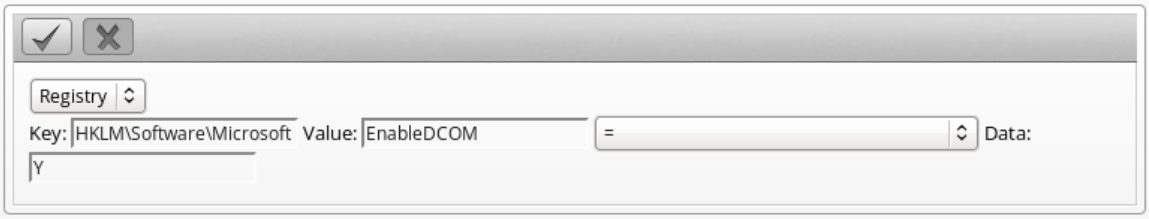
- Click **Count of** to create criteria based on the count of something, such as the number of snapshots for a virtual machine, or the number of virtual machines on a host.

- 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.



- 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.

- 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.

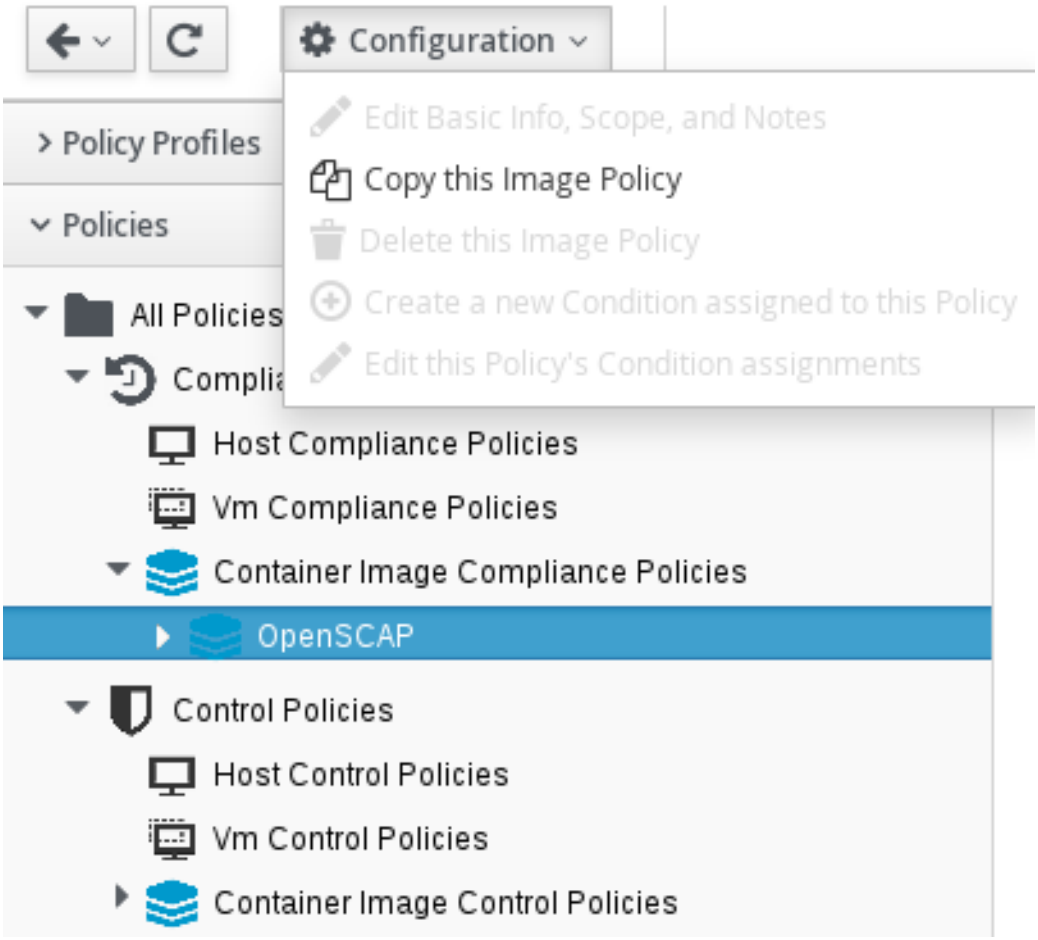


5. Click (**Commit Expression Element Changes**) to add the scope.
6. In the **Notes** area, make the required changes.
7. Click **Save**.

1.1.3. Copying a Policy

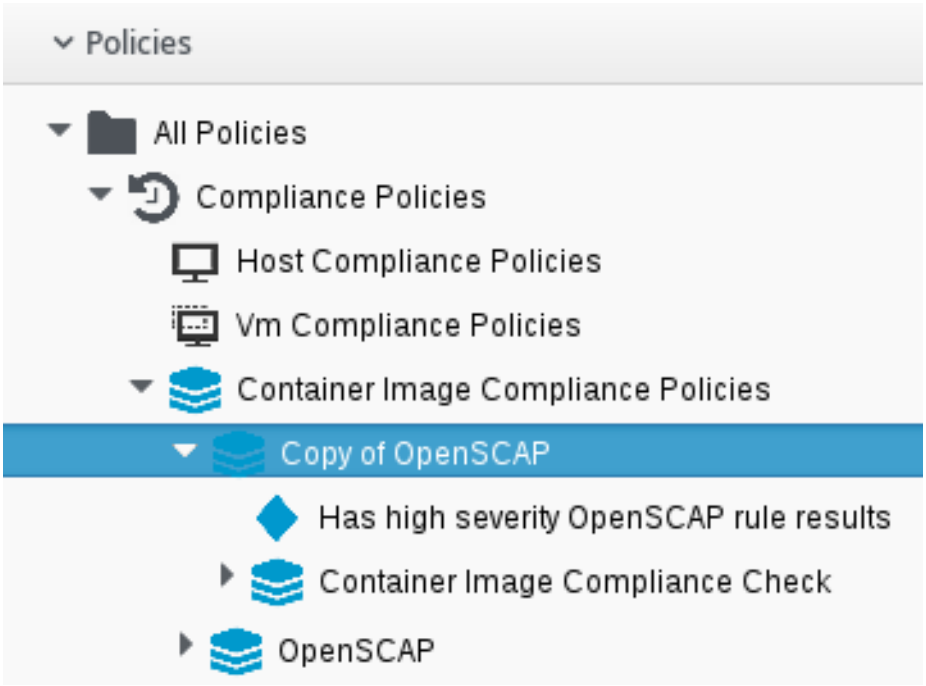
You can copy a policy if its contents are similar to a new one that you want to create, then change the condition or event associated with it. This enables you to make new policies efficiently.

1. Navigate to **Control** → **Explorer**.
2. Click the **Policies** accordion, and select the policy you want to copy.
3. Click (**Configuration**), and an option to copy the policy should appear; for example, (**Copy this Image Policy**).



4. Click **OK** to confirm.

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



1.1.4. Deleting a Policy

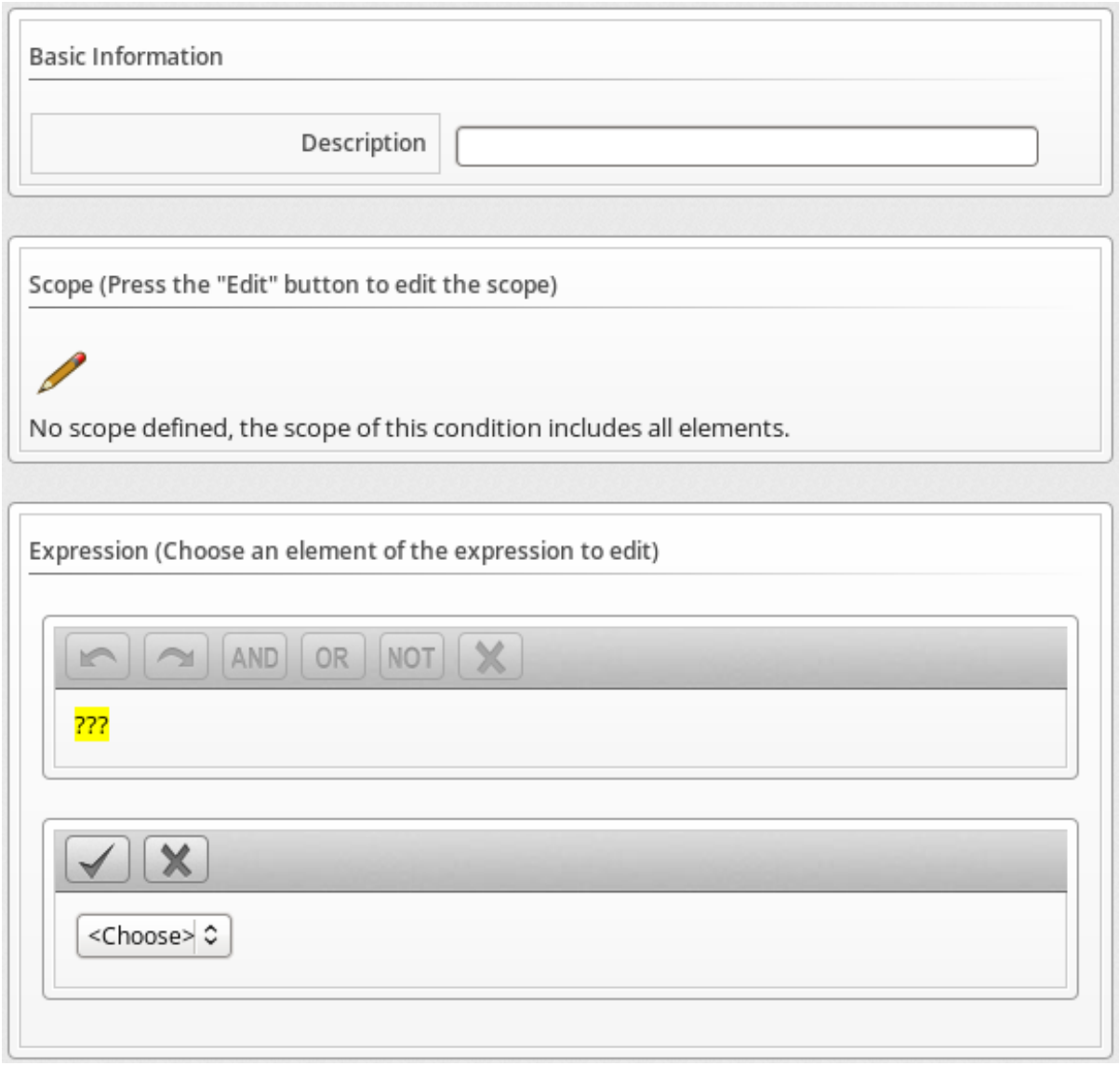
You can remove policies that you no longer need. You can only remove policies that are not assigned to a policy profile.

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/Replicator/Pod/Node/Image Policy**).
4. Click **OK** to confirm.

1.1.5. Creating a New Policy Condition

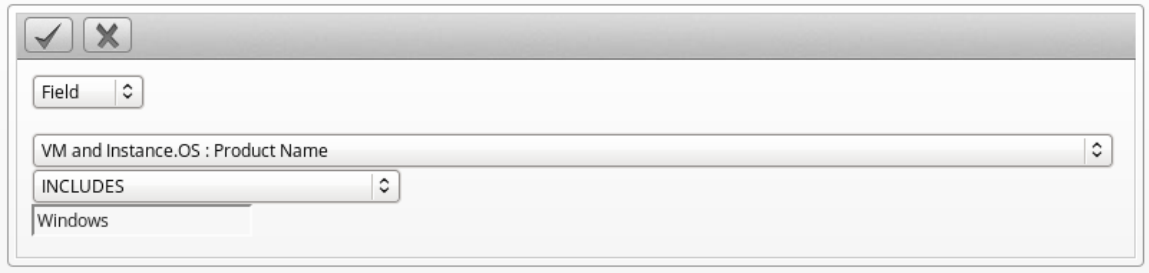
If you have not already created a condition to use with this policy, you can create one directly from inside the policy. A condition can contain two elements: a scope, and an expression. The expression is mandatory, but the scope is optional. A scope is a general attribute that is quickly checked before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

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.



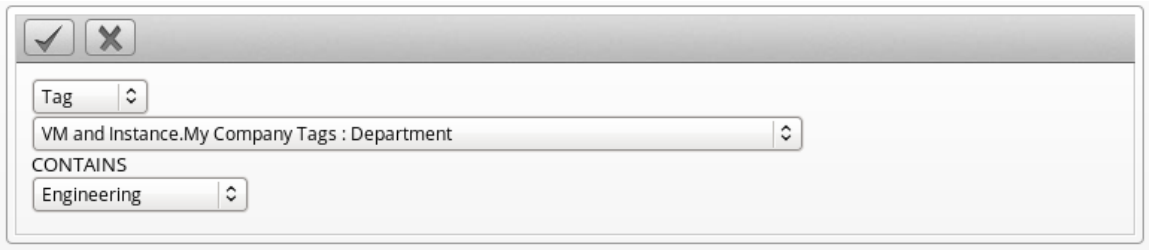
5. Click  (**Edit this Scope**) in the **Scope** area to create a general expression based on a simple attribute, such as operating system version. Based on what you choose, different options display. **Scope** is optional.

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



   - 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.

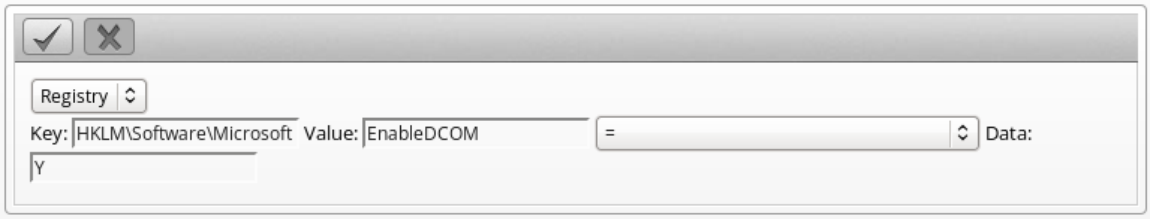
   - Click **Tag** to create criteria based on tags assigned to your resources. For example, you can check the power state of a virtual machine or see if it is tagged as production.



   - 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.

   - 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.



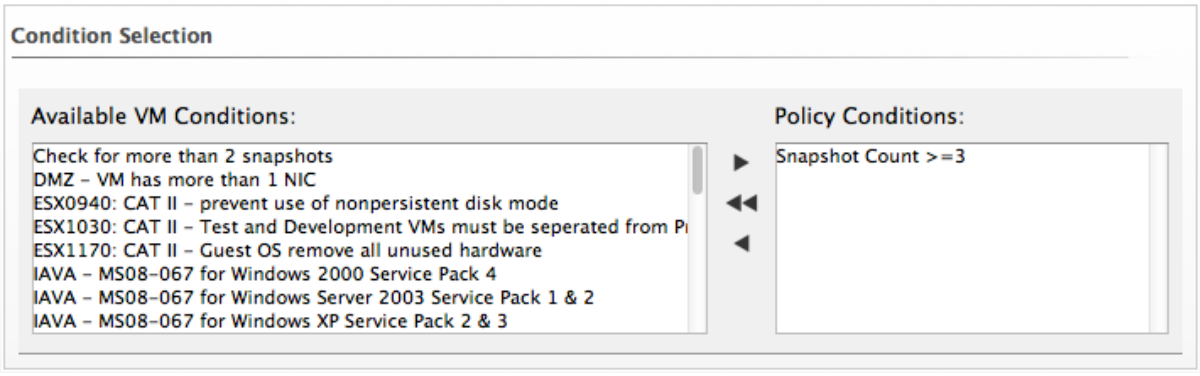
6. Click (**Commit expression element changes**) to add the scope.
7. Click (**Edit this Expression**) in the **Expression** area. Based on what you choose, options display as per the choices presented in the **Scope** area detailed above.
8. Click (**Commit Expression Element Changes**) to add the expression.
9. In **Notes**, type in a detailed explanation of the condition.
10. Click **Add**.

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

1.1.6. 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.

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.



- To add one or several 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**.

1.1.7. Editing Policy Event Assignments

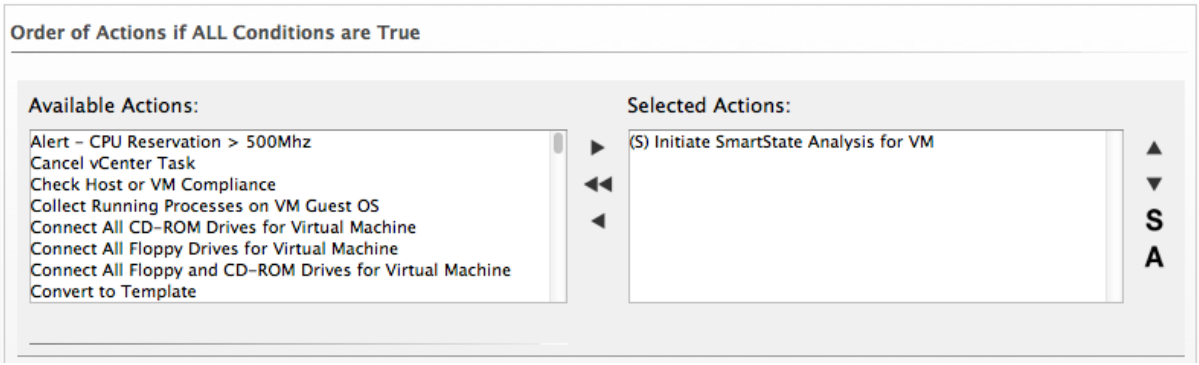
The policy evaluates its scopes and conditions when specified events occur in your virtual infrastructure. This procedure enables you to select those events and the actions that should occur based on the evaluation of the scopes and conditions for the policy.

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 Section A.1, "Events" .
5. Click **Save**.

1.1.8. Assigning an Action to an Event

This procedure describes how 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.



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 Red Hat CloudForms server in the Red Hat CloudForms 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.**

1.2. 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 entity type (virtual machine or host, for example) to which the policy applies 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 entity type and on the compare and drift screens.

1.2.1. Creating a Compliance Policy

Create compliance policies by assigning or creating a condition. Red Hat CloudForms automatically assigns the events and actions to the compliance policy as opposed to a control policy where you must define this yourself. The entity type (VM or host, for example) 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.

To create a condition, see Section 1.1.5, “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.

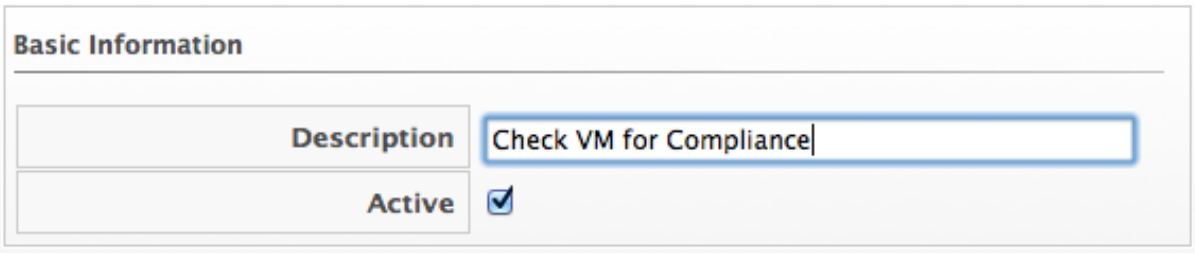
1. Navigate to **Control** → **Explorer**.

2. Click on the **Policies** accordion, and select **Compliance Policies**.

3. Select either **Host Compliance Policies** or **VM Compliance Policies** or **Replicator Compliance Policies** or **Pod Compliance Policies** or **Container Node Compliance Policies** or **Container**

Image Compliance Policies.

4. Click (**Configuration**), (**Add a new Compliance Policy**).
5. Type in a **Description** for the policy.



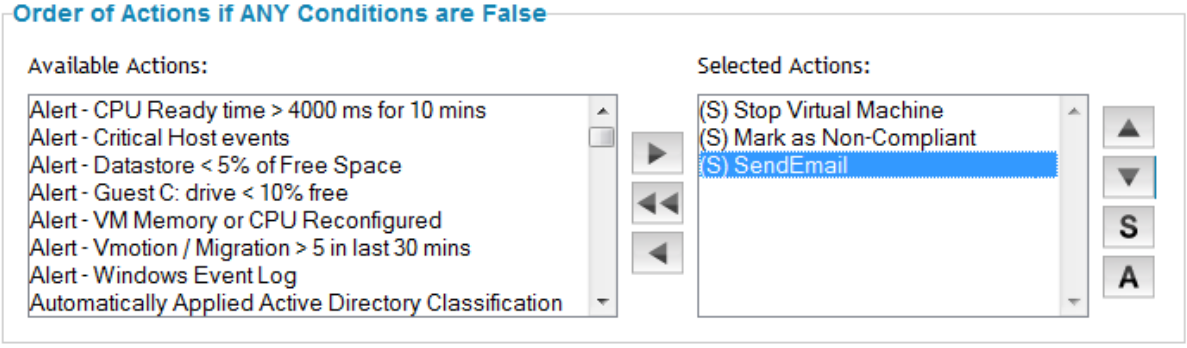
6. Uncheck **Active** if you do not want this policy processed even when assigned to a resource.
7. You can enter a scope here. (You can also create a scope as part of a condition, or not use one at all.) If the host or virtual machine is not included in the scope, no actions run.
8. In the **Notes** area, add a detailed explanation of the policy.
9. Click **Add**.

You should add one or several conditions:

- You can create a new condition by clicking (**Configuration**), (**Create a new Condition assigned to this Policy**), as described in Section 1.1.5, “Creating a New Policy Condition” .
- You can use an existing condition by clicking (**Configuration**), (**Edit this Policy's Condition assignments**), as described in Section 1.1.6, “Editing Policy Condition Assignments” .

By default, if any of the conditions are false, the virtual machine is marked as non-compliant. To add other actions, such as sending an email if the virtual machine fails the compliance test:

1. Click the **Compliance Check** event under the policy (exact name depends on entity type, for example **VM Compliance Check**).
2. Click (**Configuration**), (**Edit Actions for this Policy Event**).
3. 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.)



4. Click (**Move selected Actions into this Event**).

5. Click **Add**.

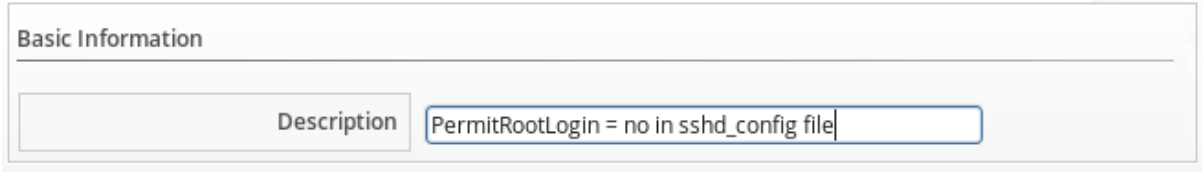
You can now make this part of a policy profile. After assigning the policy profile to the virtual machine, you can check it for its compliance status either on a schedule or on demand.

1.2.2. Creating a Compliance Condition to Check Host File Contents

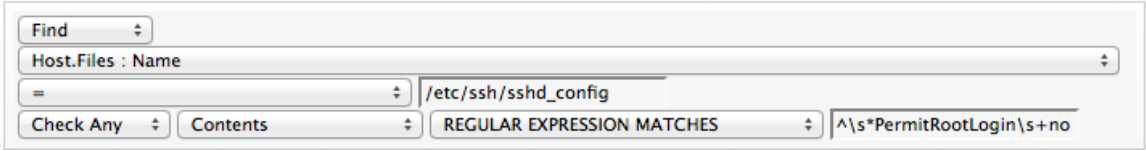
Red Hat CloudForms Control provides the ability to create a compliance condition that checks file contents. Use this to be sure that internal operating system settings meet your security criteria. Regular expressions are used to create the search pattern. Test your regular expressions thoroughly before 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 Hosts in *Managing Infrastructure and Inventory* for instructions.

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.



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`.



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**.

1.2.3. 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.

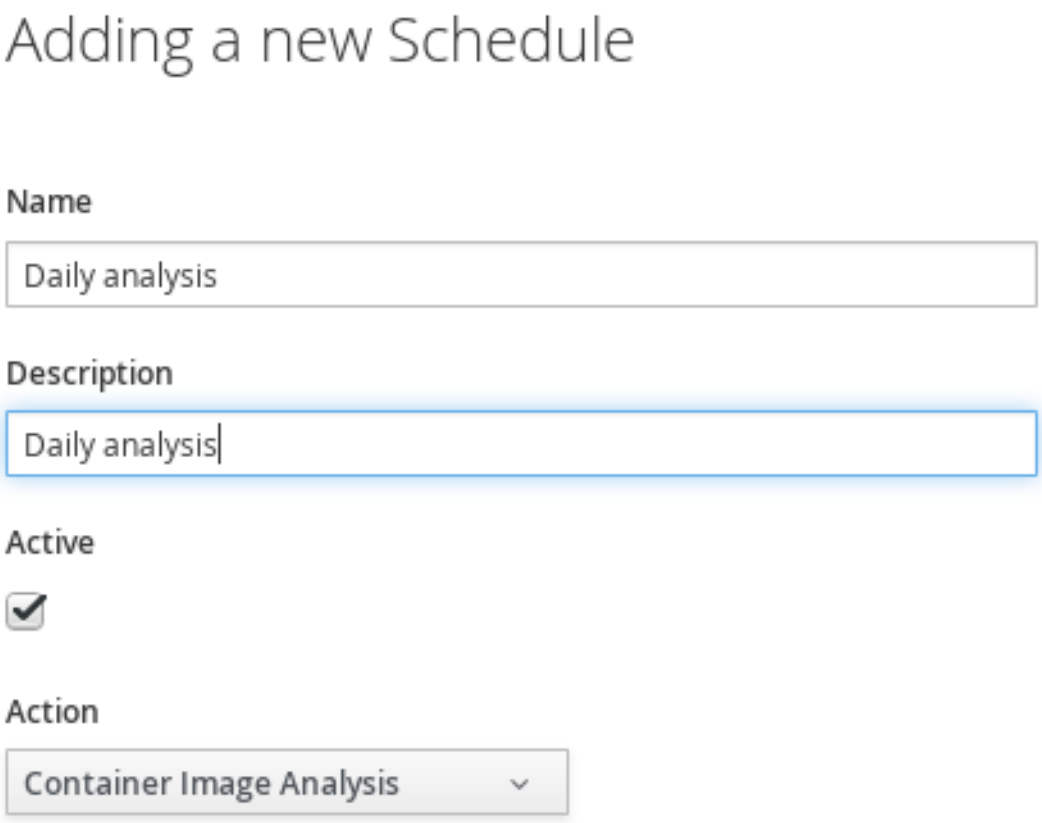
The compliance check runs all compliance policies that are assigned to the host or virtual machine. If the item fails any of the checks, it is marked as non-compliant in the item's summary screen.

NOTE

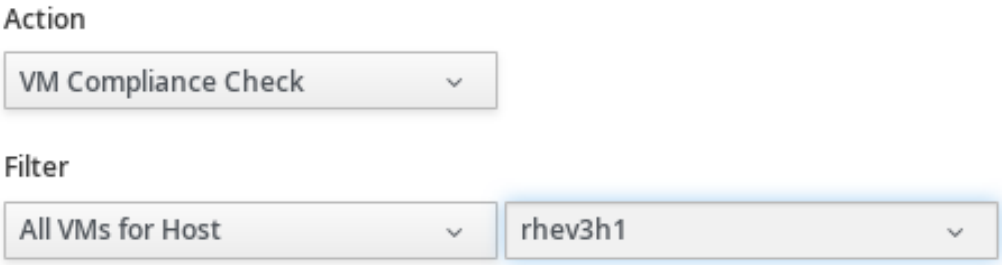
To schedule, you must have **`EvmRole-administrator`** access to the Red Hat CloudForms server.

1.2.3.1. Scheduling a Compliance Check

1. From the settings menu, select **Configuration**.
2. Click the **Settings** accordion, and select **Schedules**.
3. Click  (**Configuration**),  (**Add a new Schedule**).
4. In the **Adding a new Schedule** area, type in a name and description for the schedule.



5. Select **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.

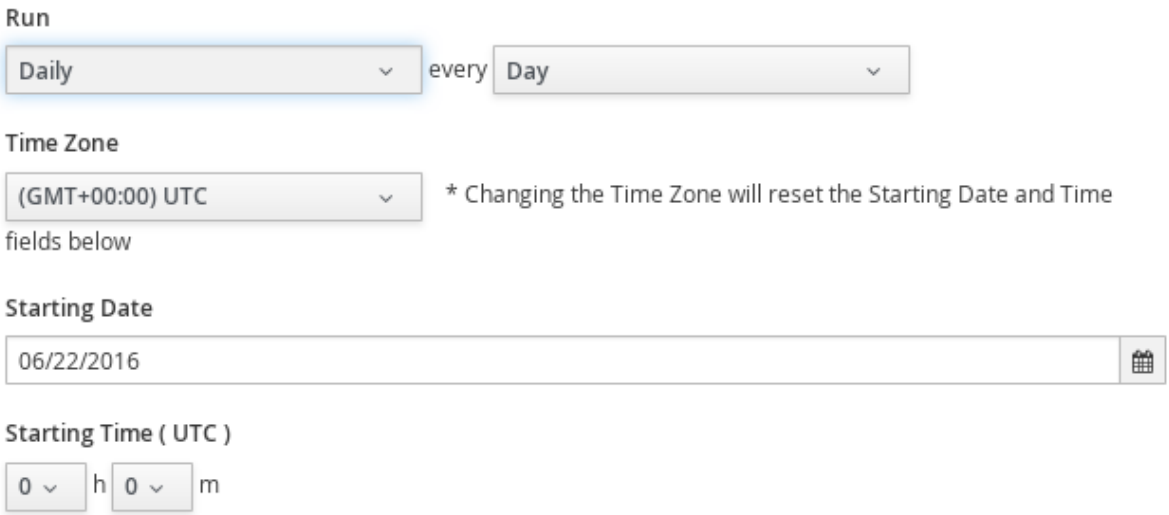


- If you choose **Host Compliance Check**, you are presented with **Host Selection** where you can choose to analyze all hosts, all hosts for a specific provider, all hosts for a cluster, a single host, or you can select hosts using a global filter.
- If you choose **Container Image Compliance Check**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

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.

1. From the **Run** dropdown, select how often you want the analysis to run. Your options after that depend on which run option you choose.



   - 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.
2. Select the time zone for the schedule.
3. Type or select a date to begin the schedule in **Starting Date**.

4. Select a starting time based on a 24-hour clock in the selected time zone.

5. Click **Add**.

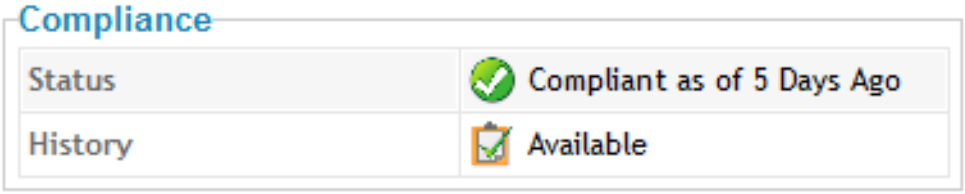
1.2.3.2. Checking a Virtual Machine for Compliance from the Summary Screen

1. Navigate to **Compute** → **Infrastructure** → **Virtual Machines**, select 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. To view the compliance history, click on the virtual machine. Under **Compliance**, if **History** is **Available**, click on it to see its compliance history.

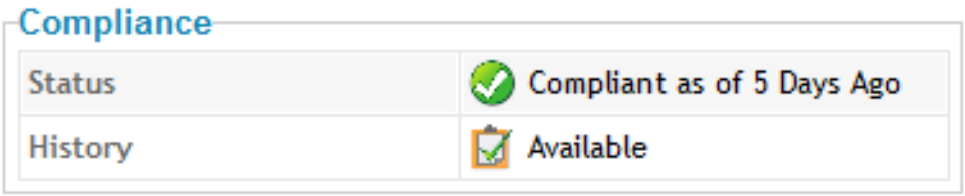


1.2.3.3. Checking a Host for Compliance from the Summary Screen

1. Navigate to **Compute** → **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**.



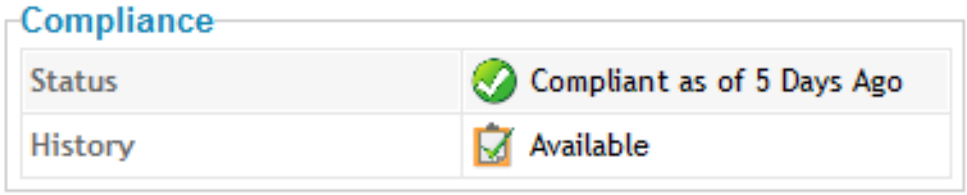
1.2.3.4. Checking a Replicator for Compliance from the Summary Screen

1. Navigate to **Compute** → **Containers** → **Replicators**, select the replicator you want to check for compliance.

2. Click (**Policy**), and then (**Check Compliance of Last Known Configuration**).

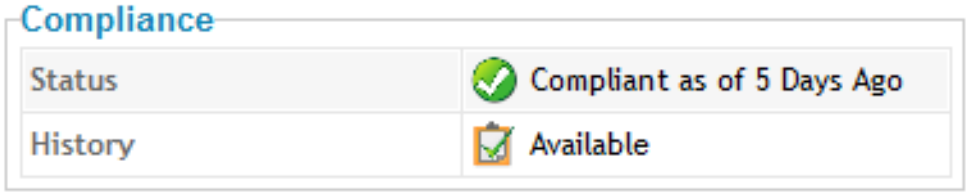
3. A confirmation message appears. Click **OK**.

4. . To view the compliance history, click on the replicator. Under **Compliance**, if **History** is **Available**, click to see its compliance history.



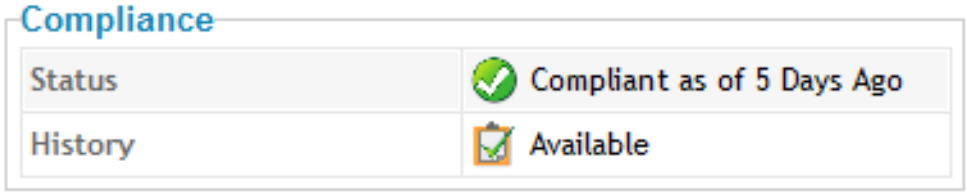
1.2.3.5. Checking a Pod for Compliance from the Summary Screen

1. Navigate to **Compute** → **Containers** → **Pods**, select the pod 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. To view the compliance history, click on the pod. Under **Compliance**, if **History** is **Available**, click to see its compliance history.



1.2.3.6. Checking a Container Node for Compliance from the Summary Screen

1. Navigate to **Compute** → **Containers** → **Container Nodes**, click the node 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. To view the compliance history, click on the node. Under **Compliance**, if **History** is **Available**, click to see its compliance history.



1.2.3.7. Checking a Container Image for Compliance from the Summary Screen

1. Navigate to **Compute** → **Infrastructure** → **Container Images**, select the container image 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. To view the compliance history, click on the container image. Under **Compliance**, if **History** is **Available**, click to see its compliance history.

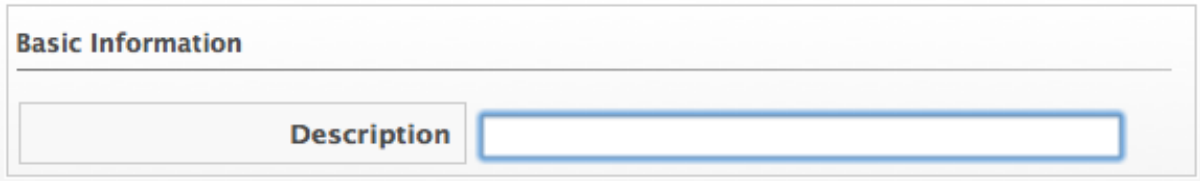
CHAPTER 2. CONDITIONS

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.

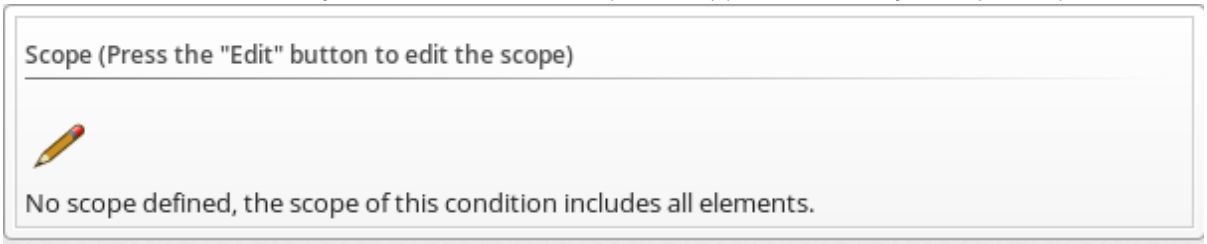
2.1. CREATING A CONDITION

You can create a condition either from within a policy screen or by going directly to the expression editor in the Red Hat CloudForms 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.

1. Navigate to **Control** → **Explorer**.
2. Click the **Conditions** accordion, and select either **Host / Node Conditions** or **VM and Instance Conditions** or **Replicator Conditions** or **Pod** or **Node Conditions** or **Image Conditions**.
3. Click  (**Configuration**), then  (**Add a New Host / VM / Replicator / Pod / Node / Image Condition**).
4. Enter a **Description** for the condition.



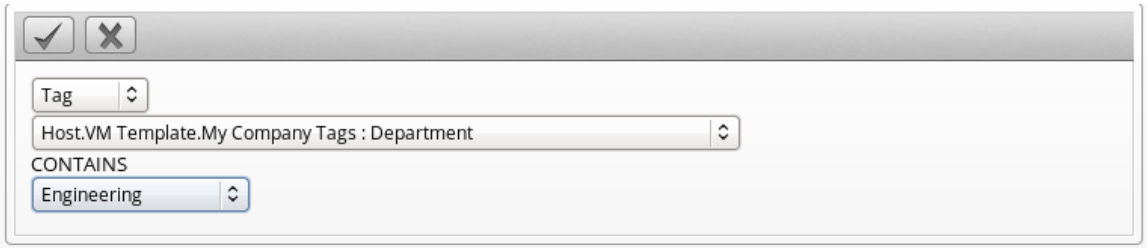
5. Click **Edit this Scope** in the **Scope** area to create a general condition based on a simple attribute. Based on what you choose, different options appear. Creating a scope is optional.



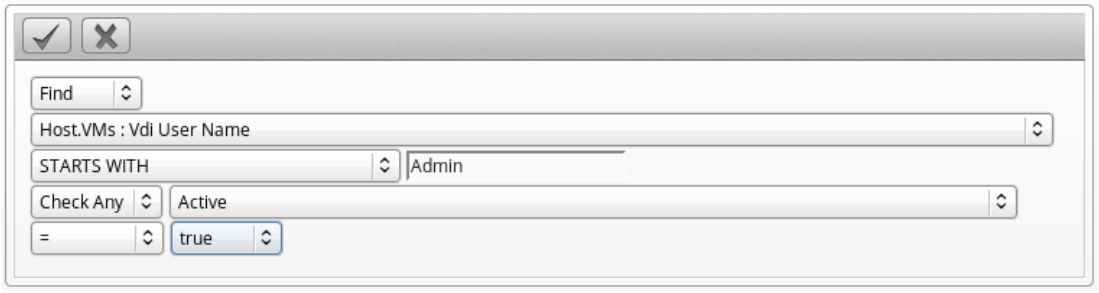
- Click **Field** to create criteria based on field values.

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

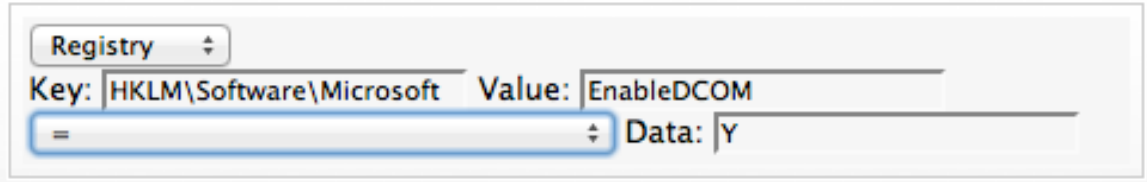
- Click **Tag** to create criteria based on tags assigned to your resources. For example, you can check the power state of a virtual machine or see if it is tagged as production.



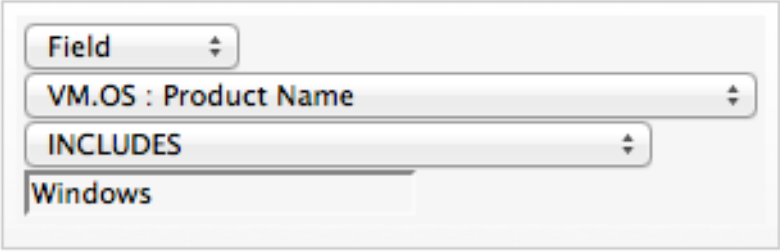
- Click **Find** to seek a particular value, and then check a property. For example, finding the Admin account and checking that it is enabled. Use the following check commands:
  - **Check Any**: The result is true if one or more of the find results satisfy the check condition.
  - **Check All**: All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



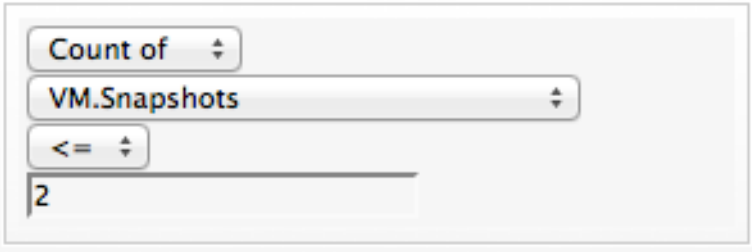
- Click **Registry** to create criteria based on registry values. For example, you can check if DCOM is enabled on a Windows System. Note that this applies only to Windows operating systems. Registry will only be available if you are creating a VM Condition.



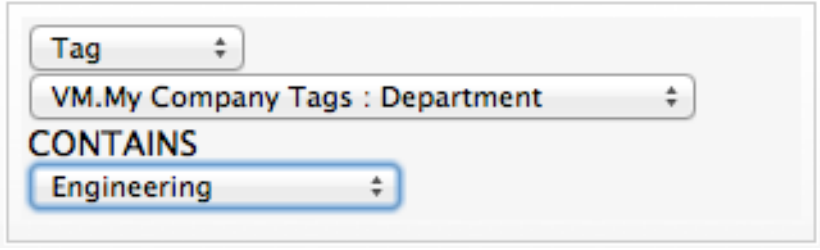
6. Click ✓ (**Commit expression element changes**) to add the scope.
7. Click **Edit this Expression** in the **Expression** area to create a general condition based on a simple attribute. Based on what you choose, different options appear.
   - Click **Field** to create criteria based on field values.



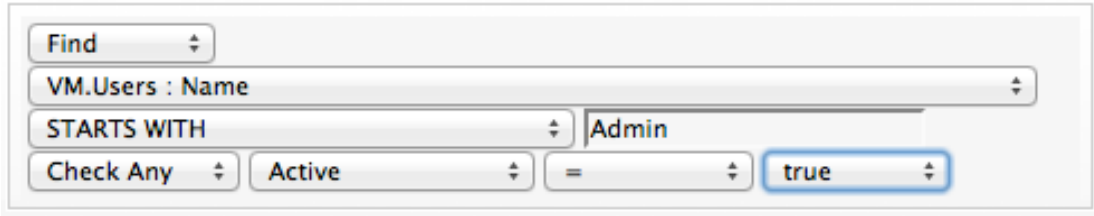
- Click **Count of** to create criteria based on the count of something, such as the number of snapshots for a virtual machine, or the number of virtual machines on a host.



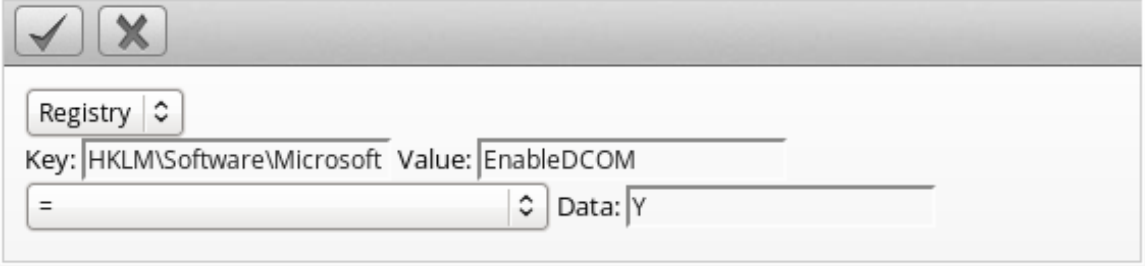
- Click **Tag** to create criteria based on tags assigned to your resources. For example, you can check the power state of a virtual machine or see if it is tagged as production.



- 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.



- 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.

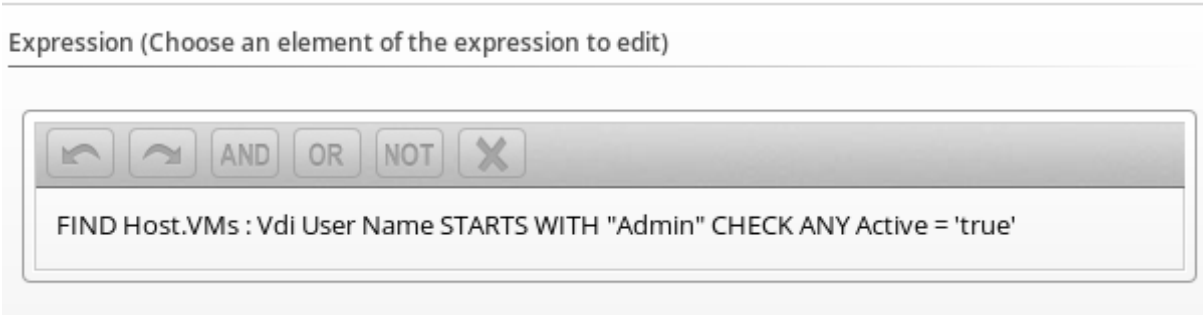


8. Click (**Commit expression element changes**) to add the expression.
9. In **Notes**, type in a detailed explanation of the condition.
10. Click **Add**.

2.2. EDITING A CONDITION

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

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.



5. Make any edits for the current expression.
   - Click (**Commit expression element changes**) to add the changes.
   - Click (**Undo the previous change**) to cancel the last action executed.
   - Click (**Redo the previous change**) to repeat the previous action executed.
   - 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**.

2.3. 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.

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**.

2.4. 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.

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 3. ACTIONS

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

Table 3.1. 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 Red Hat CloudForms log.
Initiate SmartState Analysis for Host	Start a SmartState Analysis for a host.

Action	Description
Initiate SmartState Analysis for VM	Start a SmartState Analysis for a virtual machine.
Invoke a Custom Automation	For use with Red Hat CloudForms automate. It enables you to run tasks and notifications automatically.
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 Red Hat CloudForms 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.)
Show EVM Event on Timeline	To show the EVM event on the timeline.
Shutdown Virtual Machines Guest OS	Shut down the virtual machine's operating system.
Start Virtual Machine	Power on the virtual machine.
Stop Virtual Machine	Power off the virtual machine.
Suspend Virtual Machine	Suspend the virtual machine.

3.1. CUSTOM ACTIONS

You can create a custom action using the Red Hat CloudForms 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 3.2. Custom Actions and Descriptions

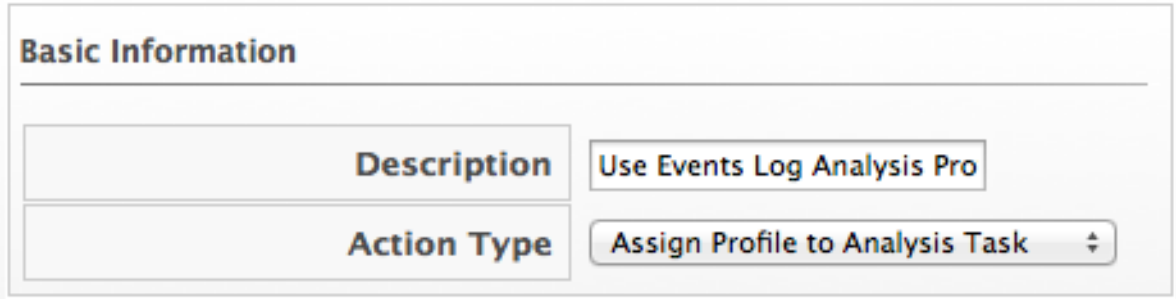
Custom Action	Description
Assign Profile to Analysis Task	When initiating a Smart State Analysis event, you can assign a specific analysis profile.

Custom Action	Description
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 Red Hat CloudForms 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.
Run Ansible Playbook	Run an Ansible playbook against an inventory selection.
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.

3.1.1. 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 Configuration in *General Configuration* for information on how to create analysis profiles.

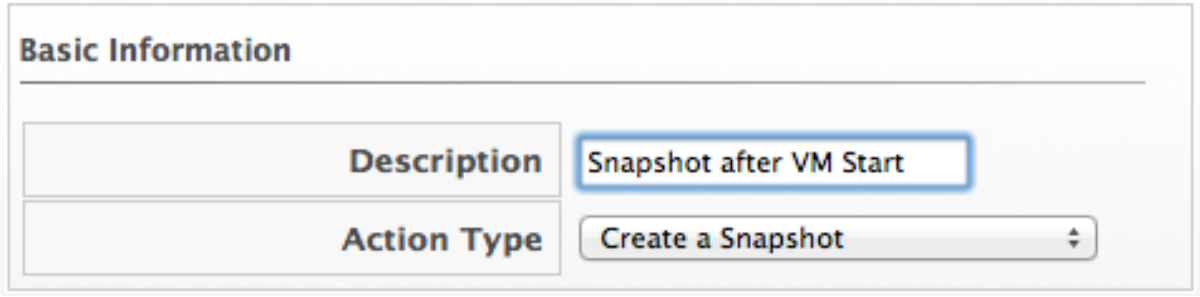
1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click  (**Configuration**),  (**Add a new Action**).
3. Type in a **Description** for the **Action Type**.



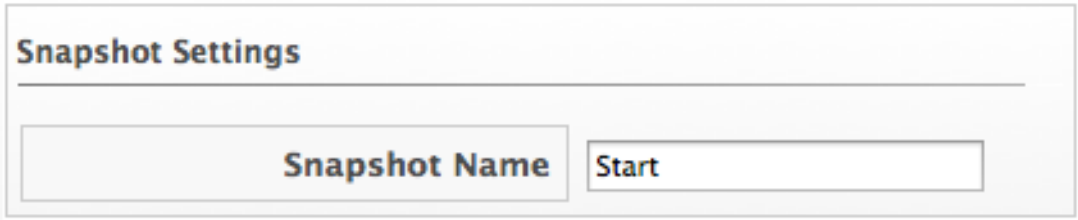
4. Select **Assign Profile to Analysis Task** from **Action Type**.
5. Select a profile from the **Analysis profiles**.
6. Click **Add**.

3.1.2. Creating 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.



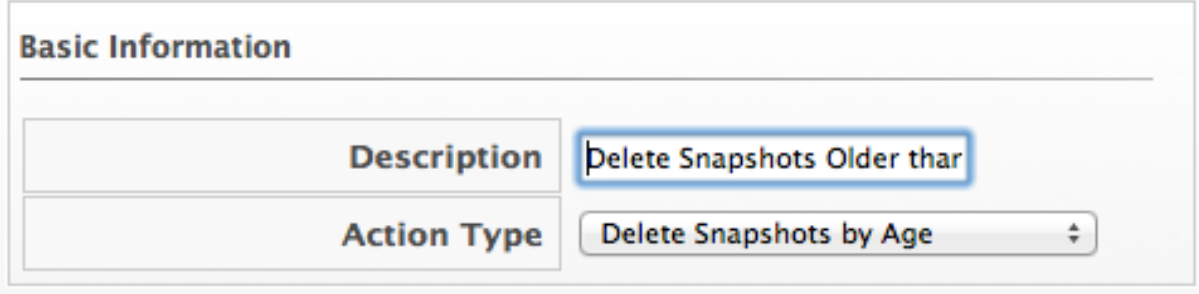
4. Select **Create a Snapshot** from **Action Type**.
5. Type in a **Snapshot Name**.



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

3.1.3. Deleting 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.

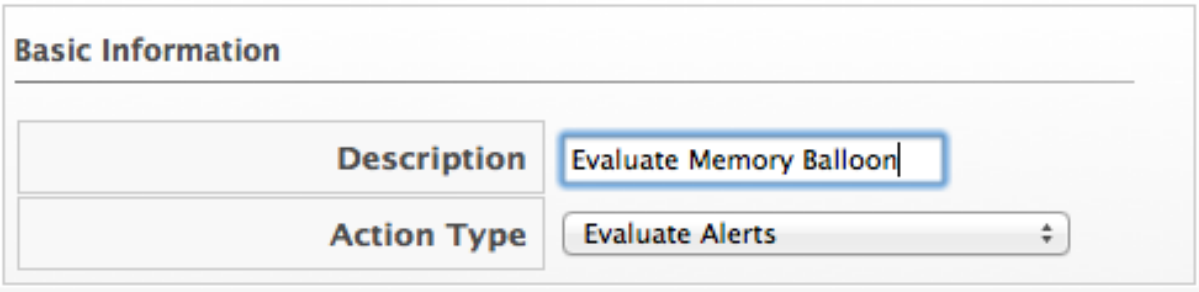


4. Select **Delete Snapshots by Age** from **Action Type**.
5. Select the age of snapshots to delete.

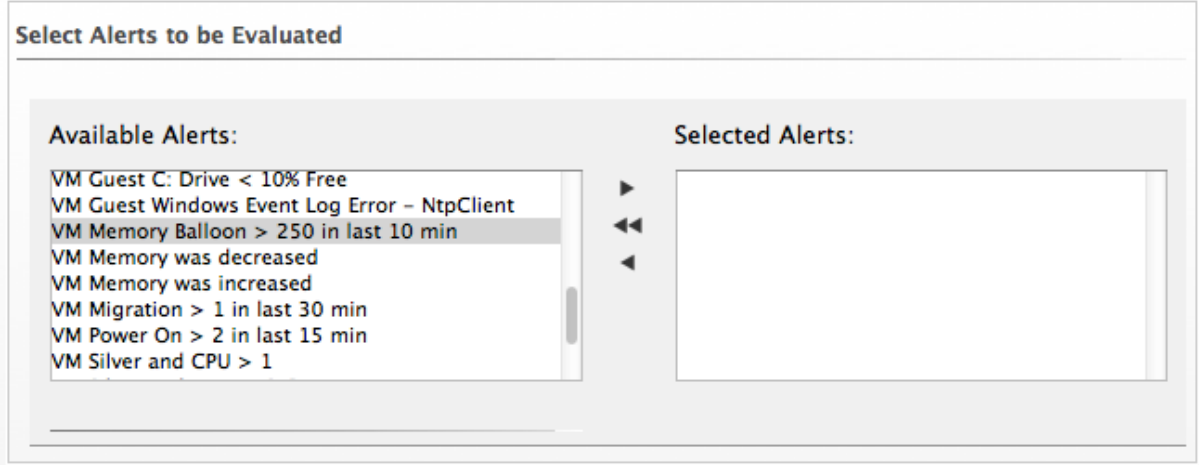
6. Click **Add**.

3.1.4. Evaluating 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.



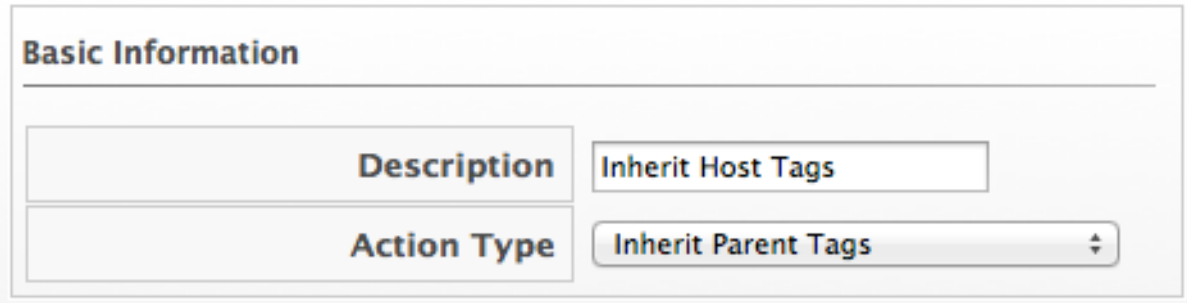
4. Select **Evaluate Alerts** from **Action Type**.
5. Select the alerts to be evaluated and click (Move selected Alerts into this Action). Use the `Ctrl` key to select multiple alerts.



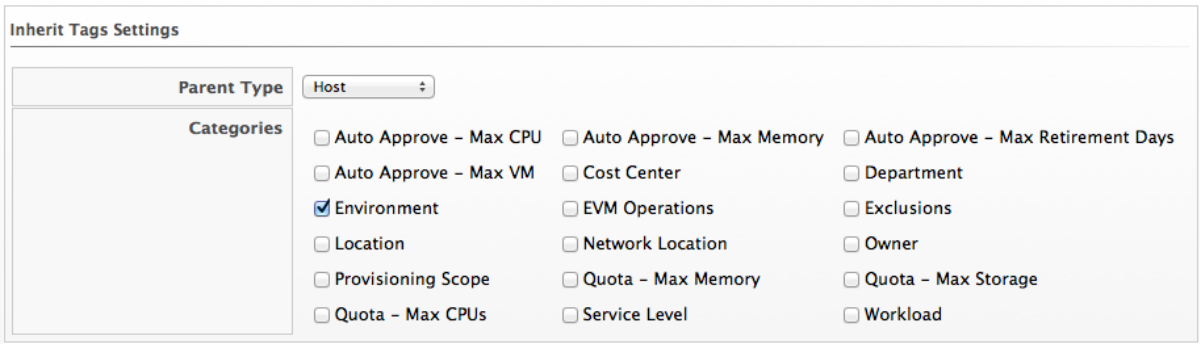
6. Click **Add**.

3.1.5. Creating 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.



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.



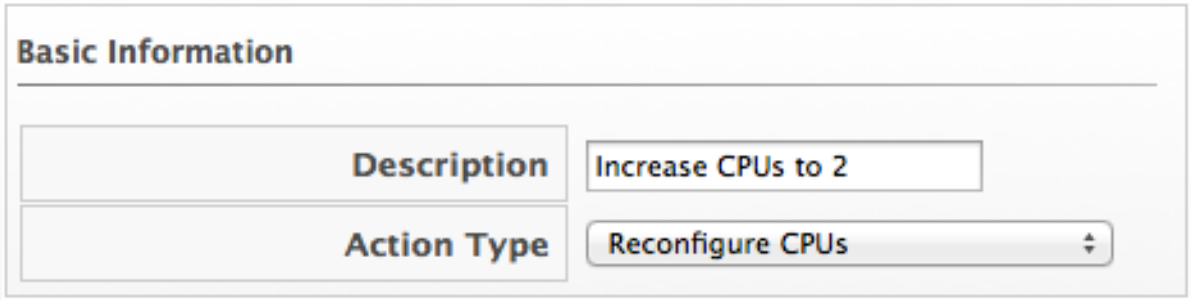
7. Click **Add**.

3.1.6. Creating a CPU Reconfigure Action

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

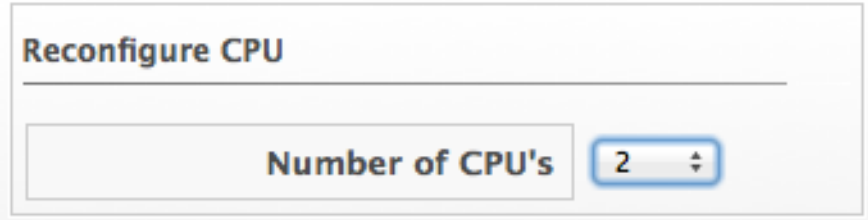
2. Click the **Actions** accordion, then click (**Configuration**), (**Add a new Action**).

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



4. Select **Reconfigure CPUs** from **Action Type**.

5. Select a number from **Number of CPUs**.



6. Click **Add**.

3.1.7. Creating a Memory Reconfigure Action

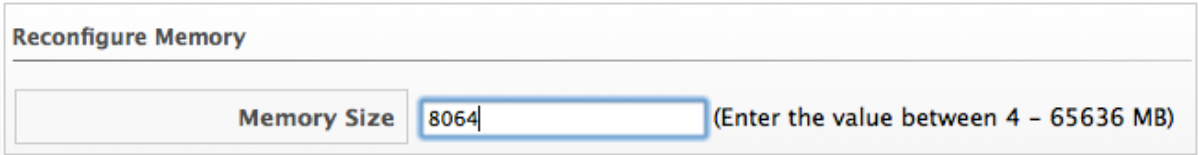
1. Navigate to **Control** → **Explorer**.

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

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

4. Select **Reconfigure Memory** from **Action Type**.

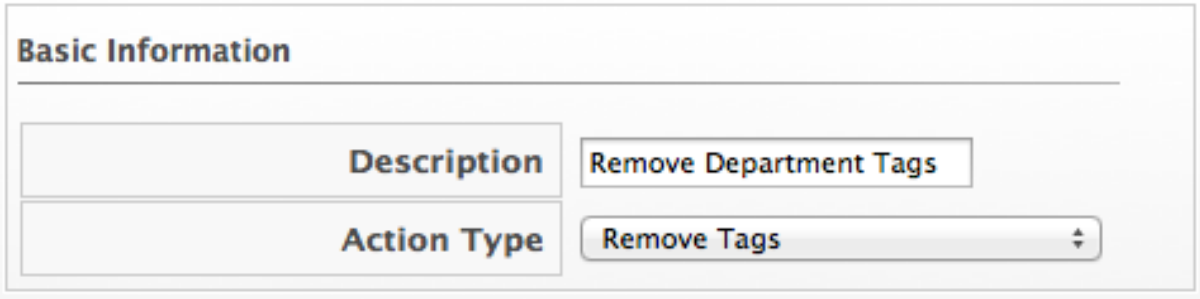
5. Type in a new value for **Memory Size**.



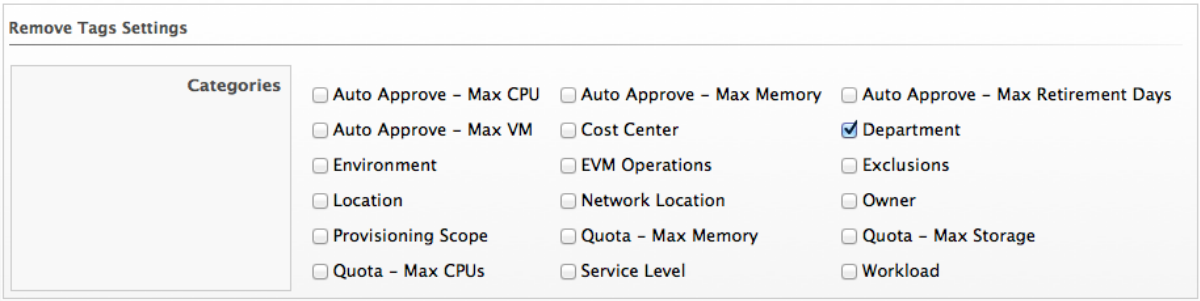
6. Click **Add**.

3.1.8. Creating 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.



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



6. Click **Add**.

3.1.9. Creating an Ansible Playbook Run Action

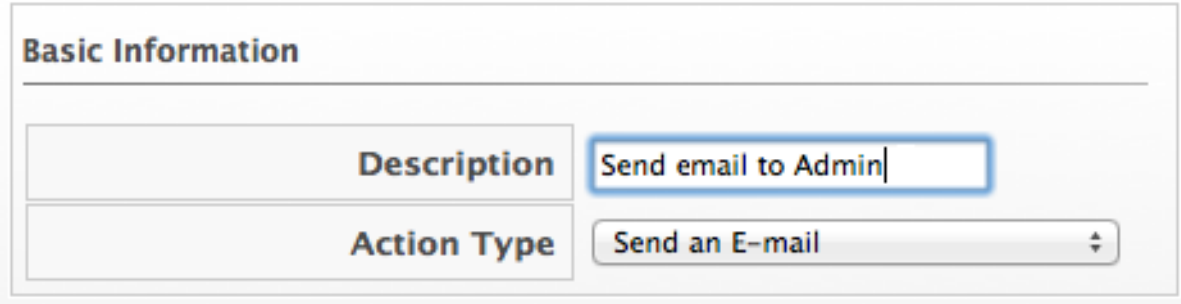
Use this action to run an Ansible Playbook against your inventory. You must first sync a playbook repository and add an Ansible Playbook service catalog item. See Automation Management Providers in *Managing Providers* for more information.

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.
4. Select **Run Ansible Playbook** from **Action Type**.
5. Select the playbook catalog item to run from **Playbook Catalog Item**.
6. Check the inventory against which you run the Ansible playbook.
   a. If **Specific Hosts** is selected, provide the IP or DNS names.
7. Click **Add**.

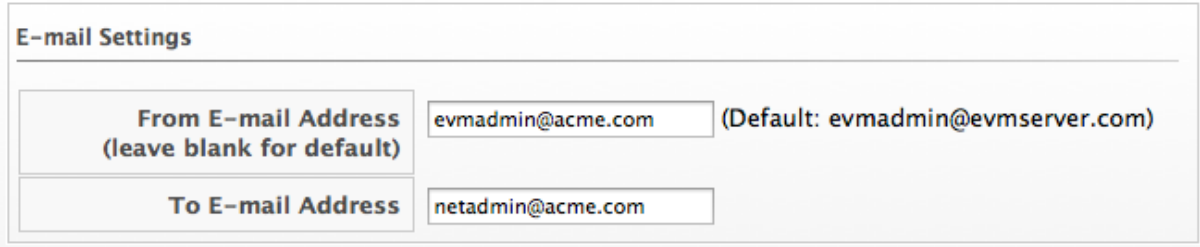
3.1.10. Creating an E-mail Action

To send emails from the Red Hat CloudForms server, you must have the notifier server role enabled and have defined settings for SMTP email. For further information regarding SMTP, see *General Configuration*.

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.



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



6. Click **Add**.

3.1.11. Creating an SNMP Action

To send SNMP traps from the Red Hat CloudForms server, you must have the `Notifier` server role and the SNMP daemons enabled. For information on enabling SNMP, see *General Configuration*.

1. Navigate to **Control** → **Explorer**.
2. Click the **Actions** accordion, then click (**Configuration**), (**Add a new Action**).
3. Enter a **Description** for the action.
4. Select **Send an SNMP** Trap from **Action Type**.
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.

     Table 3.3. 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**.

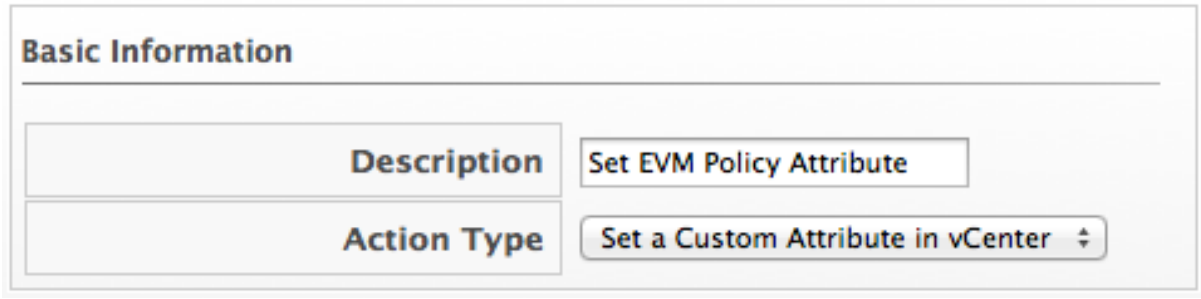
NOTE

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

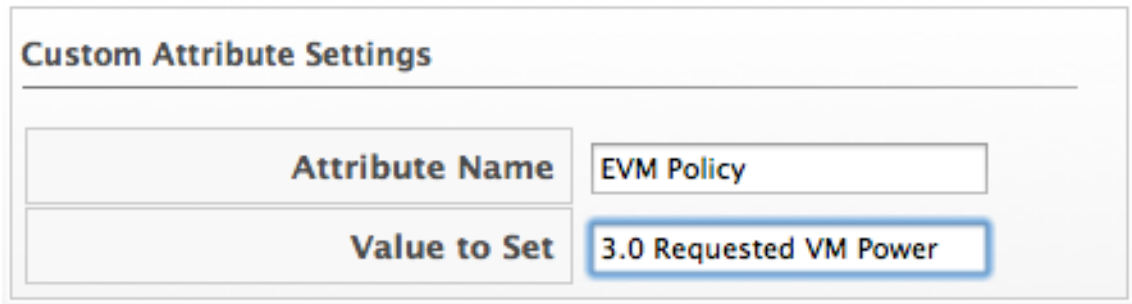
3.1.12. Creating a Set Custom Attribute Action

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

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.



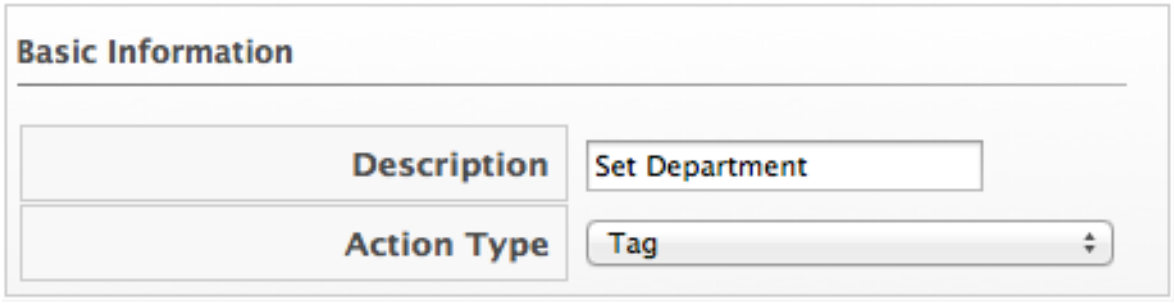
4. Select **Set a Custom Attribute in vCenter** from **Action Type**.
5. Type in the **Attribute Name** and **Value to Set**.



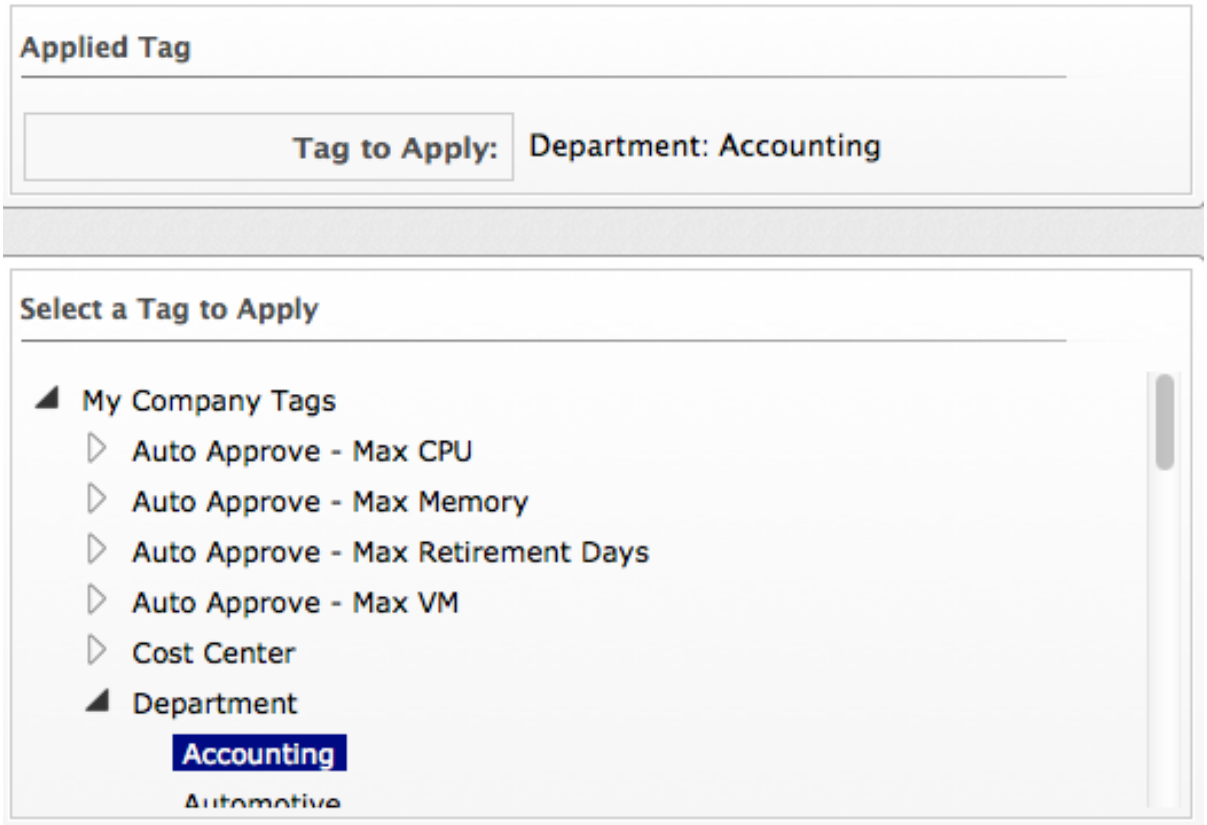
6. Click **Add**.

3.1.13. Creating 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.



4. Select **Tag** from **Action Type**.
5. Click on the appropriate tag to apply from the list provided.



6. Click **Add**.

3.2. EDITING AN ACTION

Edit an action to modify its properties. You cannot edit any of the default actions supplied with Red Hat CloudForms. 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.

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**.

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.

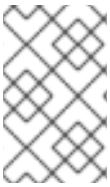
3.3. DELETING AN ACTION

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.

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 4. POLICY PROFILES

Policy profiles are groups of policies that you can assign wholesale to virtual machines, providers, clusters, hosts, resource pools, replicators, pods, container nodes, and container images. Policy profiles provide a framework for easily managing and assigning different levels of security, across various types of cloud resources.

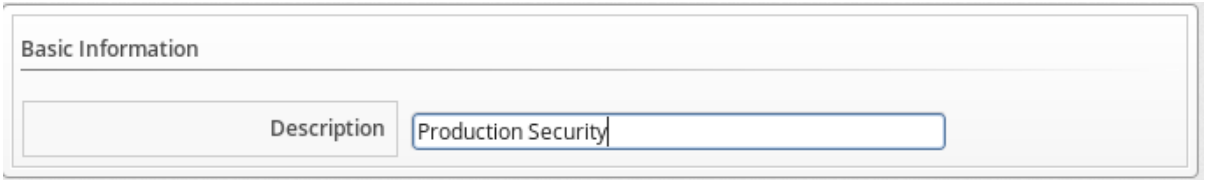


NOTE

Red Hat CloudForms also provides a built-in OpenSCAP policy profile. You can assign this profile to apply baseline security and compliance for container images. See Section A.2, “OpenSCAP Integration” for more information.

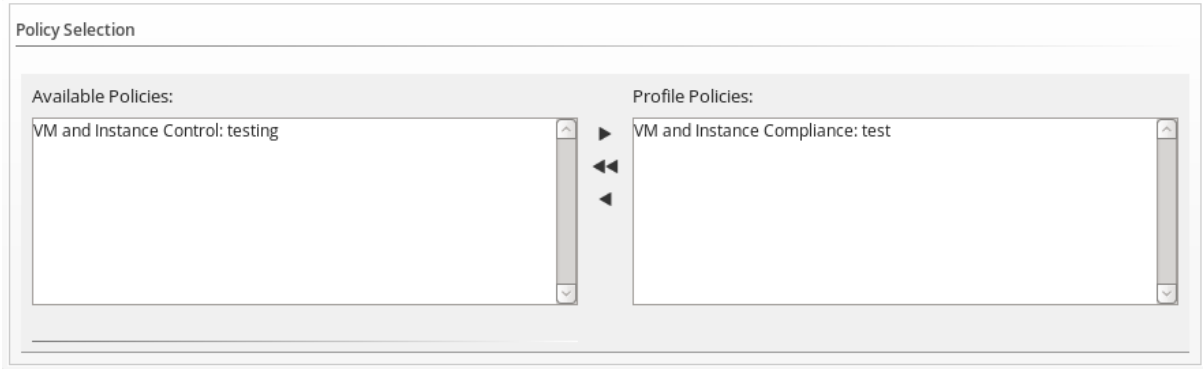
4.1. CREATING POLICY PROFILES

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.



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.

5. Click ▶ to add the **Policies**.



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

7. Click **Add**.

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.

4.2. DELETING A POLICY PROFILE

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

4.3. SIMULATING POLICY

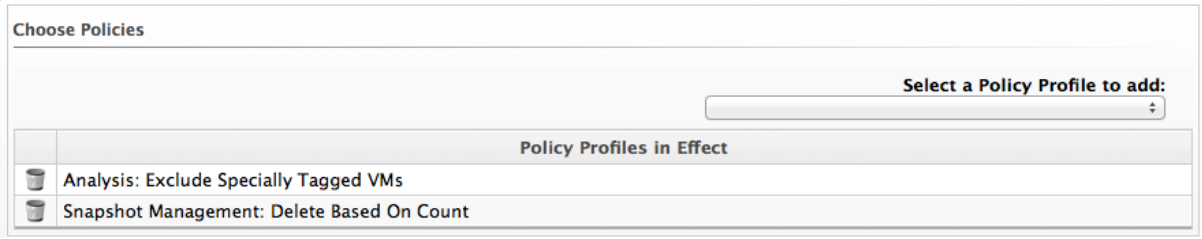
Before assigning a policy profile to a virtual machine, use the Red Hat CloudForms controls policy simulation feature to determine if a virtual machine passes a policy profile.

4.3.1. Simulating Policy Profiles on Virtual Machines

1. Navigate to **Compute** → **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.



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.

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

4.4. ASSIGNING POLICY PROFILES

After creating your policy profiles, you are ready to evaluate and assign them.

- 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, hosts, replicators, pods, container nodes or container images registered to that provider.

- Assign a policy profile to a replicator to apply the policy profile to that specific replicator.

- Assign a policy profile to a pod to apply the policy profile to that specific pod.

- Assign a policy profile to a container node to apply the policy profile to that specific node.

- Assign a policy profile to a container image to apply the policy profile to that specific image.

- 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.

4.4.1. Assigning Policy Profiles to an Infrastructure Provider

1. Navigate to **Compute** → **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**.

4.4.2. Removing Policy Profiles from an Infrastructure Provider

1. Navigate to **Compute** → **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**.

4.4.3. Assigning Policy Profiles to a Cluster

1. Navigate to **Compute** → **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**.

4.4.4. Removing Policy Profiles from a Cluster

1. Navigate to **Compute** → **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**.

4.4.5. Assigning Policy Profiles to a Host

1. Navigate to **Compute** → **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**.

4.4.6. Removing Policy Profiles from a Host

1. Navigate to **Compute** → **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**.

4.4.7. Assigning Policy Profiles to a Virtual Machine

1. Navigate to **Compute** → **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**.

4.4.8. Removing Policy Profiles from a Virtual Machine

1. Navigate to **Compute** → **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**.

4.4.9. Assigning Policy Profiles to a Resource Pool

1. Navigate to **Compute** → **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**.

4.4.10. Removing Policy Profiles from a Resource Pool

1. Navigate to **Compute** → **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**.

4.4.11. Assigning Policy Profiles to a Cloud Provider

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

4.4.12. Removing Policy Profiles from a Cloud Provider

1. Navigate to **Compute** → **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**.

4.4.13. Assigning Policy Profiles to a Network Provider

1. Navigate to **Networks** → **Providers**, check the network 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**.

4.4.14. Removing Policy Profiles from a Network Provider

1. Navigate to **Networks** → **Providers**, check the network providers 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 profile you need to remove. It turns blue to show that its assignment state has changed.
5. Click **Save**.

4.4.15. Assigning Policy Profiles to a Container Provider

1. Navigate to **Compute** → **Containers** → **Providers** and select 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 and see its member policies.
4. Select the policy profiles you need to apply to the provider. It will turn blue to show the selection.
5. Click **Save**.

4.4.16. Removing Policy Profiles from a Container Provider

1. Navigate to **Compute** → **Containers** → **Providers**, select the container providers 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 profile you need to remove. It turns blue to show that its assignment state has changed.

5. Click **Save**.

4.4.17. Assigning Policy Profiles to a Replicator

1. Navigate to **Compute** → **Containers** → **Replicators** and select the replicator 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 and see its member policies.

4. Select the policy profiles you need to apply to the replicator. It will turn blue to show the selection.

5. Click **Save**.

4.4.18. Removing Policy Profiles from a Replicator

1. Navigate to **Compute** → **Containers** → **Replicators**, select the replicators 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 profile you need to remove. It turns blue to show that its assignment state has changed.

5. Click **Save**.

4.4.19. Assigning Policy Profiles to a Pod

1. Navigate to **Compute** → **Containers** → **Pods** and select the pod 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 and see its member policies.

4. Select the policy profiles you need to apply to the pod. It will turn blue to show the selection.

5. Click **Save**.

4.4.20. Removing Policy Profiles from a Pod

1. Navigate to **Compute** → **Containers** → **Pods**, select the pods 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 profile you need to remove. It turns blue to show that its assignment state has changed.
5. Click **Save**.

4.4.21. Assigning Policy Profiles to a Container Node

1. Navigate to **Compute** → **Containers** → **Container Nodes** and select the container node 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 and see its member policies.
4. Select the policy profiles you need to apply to the node. It will turn blue to show the selection.
5. Click **Save**.

4.4.22. Removing Policy Profiles from a Container Node

1. Navigate to **Compute** → **Containers** → **Container Nodes**, select the container nodes 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 profile you need to remove. It turns blue to show that its assignment state has changed.
5. Click **Save**.

4.4.23. Assigning Policy Profiles to a Container Image

1. Navigate to **Compute** → **Containers** → **Container Images** and select the image 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 and see its member policies.
4. Select the policy profiles you need to apply to the image. It will turn blue to show the selection.

5. Click **Save**.

4.4.24. Removing Policy Profiles from a Container Image

1. Navigate to **Compute** → **Containers** → **Container Images**, select the container images 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 profile you need to remove. It turns blue to show that its assignment state has changed.
5. Click **Save**.

4.4.25. Assigning Policy Profiles to an Instance

1. From **Compute** → **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**.

4.4.26. Removing Policy Profiles from an Instance

1. Navigate to **Compute** → **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**.

4.5. 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.

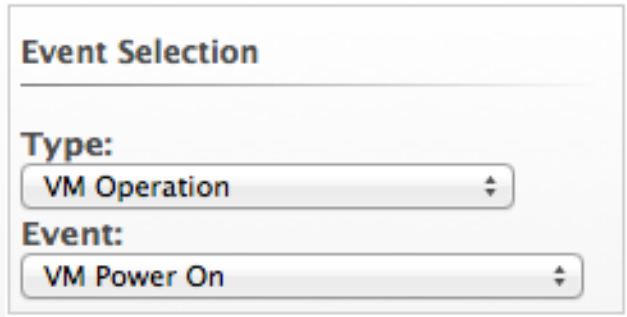
1. Navigate to **Control** → **Explorer**.

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**.

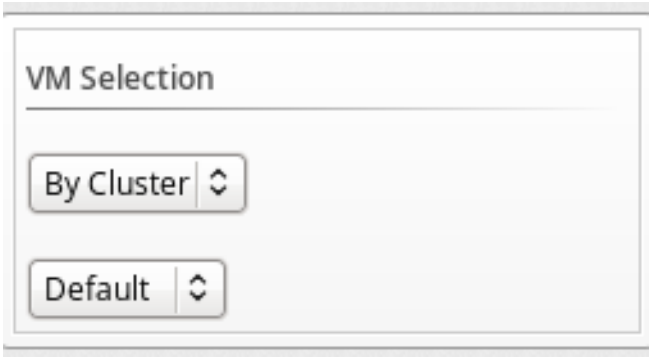
4.6. VIEWING POLICY SIMULATION - RESULTANT SET OF POLICY (RSOP)

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 Red Hat CloudForms console.

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.



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



4. Click **Submit**.

APPENDIX A. APPENDIX

A.1. EVENTS

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

Table A.1. Event Types

Category	Description
Container Operation	Events related to container analysis.
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 virtual machine discovery, provisioning, and virtual machine 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, shutdown, and suspend.
Service Lifecycle	Events associated with service lifecycle. These include, but are not limited to, provisioning completed, start request, started, stop request, stopped, retirement warning, and retired.

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

Table A.2. Events and Descriptions

Event	Description
Container Image Analysis Complete	Check the condition when an analysis of a container image completes.
Container Image Discovered	Check the condition when a new container image is discovered.
Container Image Compliance Check	Check the condition when a compliance check is performed on an image.
Container Image Compliance Passed	Check the condition when an image passes a compliance check.
Container Image Compliance Failed	Check the condition when an image fails a compliance check.
Container Node Failed Mount	Check the condition when a node fails to mount a volume for a pod.
Container Node Invalid Disk Capacity	Check the condition when a node's disk capacity is invalid.
Container Node Not Ready	Check the condition when a node is not ready.
Container Node Not Schedulable	Check the condition when a node is not schedulable.
Container Node Ready	Check the condition when a node is ready.
Container Node Schedulable	Check the condition when a node is schedulable.
Container Node Rebooted	Check the condition when a node reboots.
Container Node Compliance Check	Check the condition when a compliance check is performed on a node.
Container Node Compliance Passed	Check the condition when a node passes a compliance check.
Container Node Compliance Failed	Check the condition when a node fails a compliance check.
Pod Deadline Exceeded	Check the condition when a pod with specified deadline exceeds it and is terminated.
Pod Failed Scheduling	Check the condition when scheduling a pod fails.

Event	Description
Pod Failed Sync	Check the condition when getting a pod to its desired state fails (a frequent reason is failure to download the image).
Pod Failed Validation	Check the condition when a pod validation fails.
Pod hostPort Conflict	Check the condition when a pod hostPort conflict occurs.
Pod Insufficient Free CPU	Check the condition when there is an insufficient free CPU in a pod.
Pod Insufficient Free Memory	Check the condition when there is an insufficient free memory in a pod.
Pod nodeSelector Mismatching	Check the condition when a pod nodeSelector mismatches.
Pod Out of Disk	Check the condition when a pod is out of disk space.
Pod Scheduled	Check the condition when a pod is scheduled onto the node.
Pod Compliance Check	Check the condition when a compliance check is performed on a pod.
Pod Compliance Passed	Check the condition when a pod passes a compliance check.
Pod Compliance Failed	Check the condition when a pod fails a compliance check.
Replicator Failed Creating Pod	Check the condition when a replicator fails creating a pod.
Replicator Successfully Created Pod	Check the condition when a replicator successfully creates a pod.
Replicator Compliance Check	Check the condition when a compliance check is performed on a replicator.
Replicator Compliance Passed	Check the condition when a replicator passes a compliance check.
Replicator Compliance Failed	Check the condition when a replicator fails a compliance check.

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 user interface.
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 Red Hat CloudForms console.
Host Auth Changed	Check the condition when host authentication credentials are changed in the Red Hat CloudForms 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.
Host Auth Incomplete Credentials	Check the condition if host authentication credentials are not complete in the user interface.
Host Auth Invalid	Check the condition if Red Hat CloudForms is able to communicate with the host and the credentials fail.
Host Auth Unreachable	Check the condition if Red Hat CloudForms is unable to communicate with the host.
Host Auth Valid	Check the condition when the host authentication credentials entered in the Red Hat CloudForms 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.

Event	Description
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 Red Hat CloudForms automate, for future use in policies.* Check the condition when provider authentication credentials are changed in the user interface.
Provider Auth Error	*For use only with Red Hat CloudForms 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 automate, for future use in policies.* Check the condition if provider authentication credentials are not complete in the Red Hat CloudForms console.
Provider Auth Invalid	*For use only with Red Hat CloudForms automate, for future use in policies.* Check the condition if Red Hat CloudForms is able to communicate with the provider and the credentials fail.
Provider Auth Unreachable	*For use only with automate, for future use in policies.* Check the condition if Red Hat CloudForms is unable to communicate with the provider.
Provider Auth Valid	*For use only with Red Hat CloudForms automate, for future use in policies.* Check the condition when the provider authentication credentials entered in the user interface are valid.
Provider Compliance Check	Check the condition when a compliance check is performed on a provider.
Provider Compliance Failed	Check the condition when a provider fails a compliance check.

Event	Description
Provider Compliance Passed	Check the condition when a provider passes a compliance check.
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 a virtual machine's parent cluster.
Tag Parent Datastore Complete	Check the condition after a company tag is assigned to a virtual machine's parent datastore.
Tag Parent Host Complete	Check the condition after a company tag is assigned to a virtual machine's parent host.
Tag Parent Resource Pool Complete	Check the condition after a company tag is assigned to a virtual machine's 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 a virtual machine's parent cluster.

Event	Description
Un-Tag Parent Datastore Complete	Check the condition after a company tag is removed from a virtual machine's parent datastore.
Un-Tag Parent Host Complete	Check the condition after a company tag is removed from a virtual machine's parent host.
Un-Tag Parent Resource Pool Complete	Check the condition after a company tag is removed from a virtual machine's 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.
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 Red Hat CloudForms 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 virtual machine.

Event	Description
VM Compliance Failed	Check the condition when a virtual machine fails a compliance check.
VM Compliance Passed	Check the condition when a virtual machine 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 user interface.
VM Guest Reboot	Check the condition when a virtual machine is rebooted.
VM Guest Reboot Request	Check the condition when someone tries to reboot a virtual machine from the Red Hat CloudForms 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 shut down the operating system of a virtual machine from the user interface.
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 Red Hat CloudForms console.
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 Red Hat CloudForms console.
VM Provision Complete	Check the condition when a virtual machine is provisioned.
VM Remote Console Connected	Check the condition when a virtual machine is connected to a remote console.

Event	Description
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 Red Hat CloudForms console to unregister a virtual machine.
VM Renamed Event	Check the condition when a virtual machine is renamed on its provider.
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 Red Hat CloudForms console.
VM Retire Request	Check the condition when a virtual machine retirement request is created from Red Hat CloudForms.
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 user interface.
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 Red Hat CloudForms console.
VM Suspend	Check the condition when a virtual machine is suspended.

Event	Description
VM Suspend Request	Check the condition when someone tries to suspend a virtual machine from the Red Hat CloudForms console.
VM Template Create Complete	Check the condition when a virtual machine template is created.

A.2. OPENSCAP INTEGRATION

OpenSCAP is an auditing tool used for hardening the security of your enterprise. This tool is built upon the knowledge and resources provided by the many experienced security experts active in the upstream OpenSCAP ecosystem. For more information about OpenSCAP, see https://www.open-scap.org/.

Red Hat CloudForms now supports OpenSCAP. By default, Red Hat CloudForms provides a built-in *OpenSCAP policy profile* which provides policies for managing the security of your *container images*.

These policies ensure that new container images from any provider within Red Hat CloudForms are scanned against the latest CVE content from Red Hat. See Red Hat's Security Data page for more details about this content. In particular, the SCAP source data stream files index provides examples of security advisories used by the built-in OpenSCAP policy profile.

Each of these security advisories have a severity ranging from **Low** to **Critical**. With the built-in OpenSCAP policy profile, any image that fails a security check against an advisory with at least a **High** severity is marked as non-compliant.

The built-in OpenSCAP policy profile cannot be edited. You can, however, edit copies of its policies and assign those copies to a new profile. See Section A.3, "Creating a Customized OpenSCAP Policy Profile" for more information.

A.2.1. Assigning the Built-In OpenSCAP Policy Profile

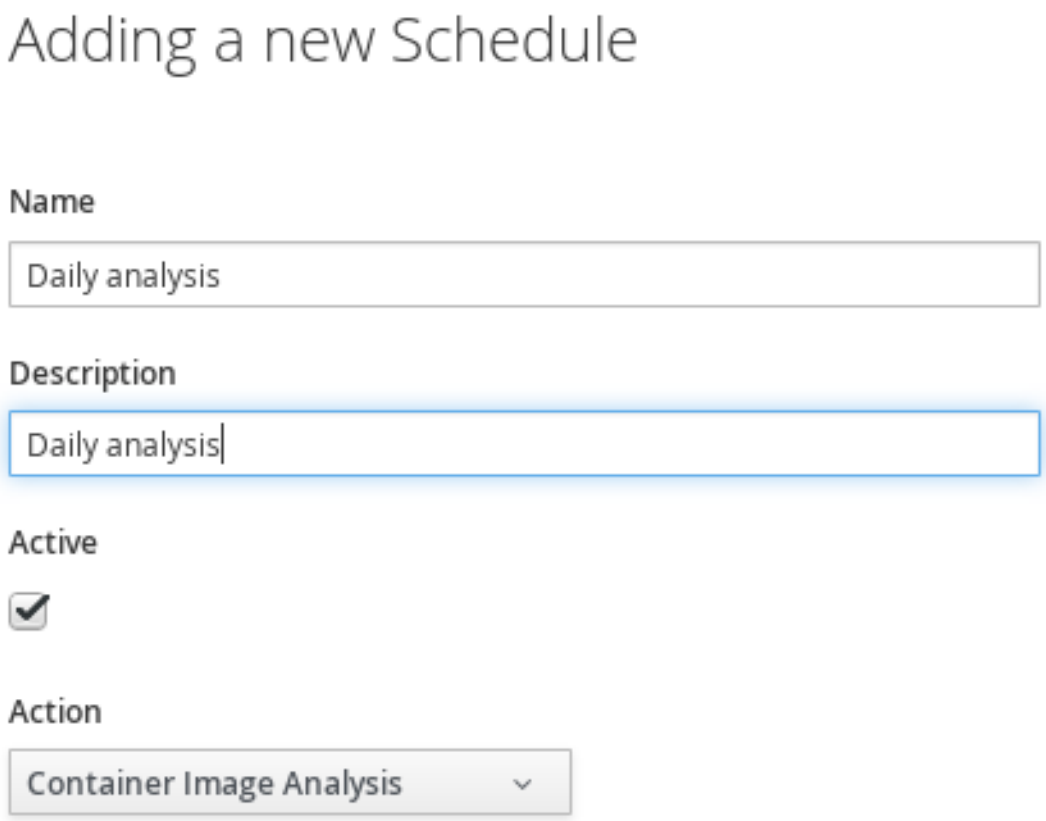
The OpenSCAP policy profile included with Red Hat CloudForms is not automatically assigned. You still need to assign it to a container provider. The method for doing so is similar to that of any normal policy profile (as in Section 4.4, "Assigning Policy Profiles"):

1. Navigate to **Compute** → **Containers** → **Providers**, check the providers you need to assign the OpenSCAP policy profile to.
2. Click  (**Policy**), and then click  (**Manage Policies**).
3. From the **Select Policy Profiles** area, click on the triangle next to **OpenSCAP profile** to expand it and see its member policies.
4. Check **OpenSCAP profile**. It turns blue to show its assignment state has changed.
5. Click **Save**.

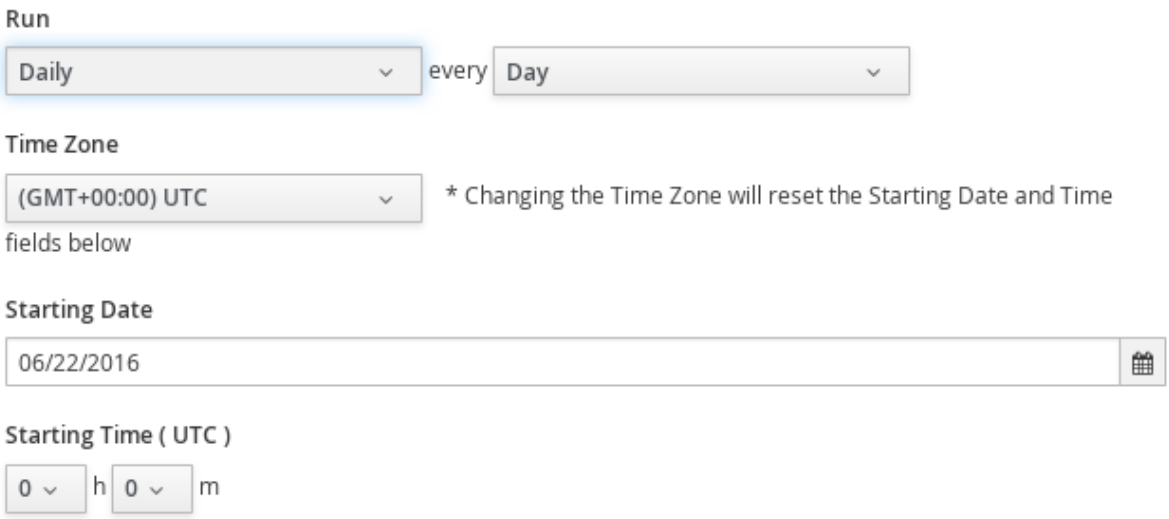
A.2.2. Scheduling an OpenSCAP Compliance Check on Container Images

Once you have assigned the built-in OpenSCAP policy profile to a container provider, you can schedule a compliance check against the policy profile. The method for doing is similar to that of scheduling a normal compliance check (Section 1.2.3.1, “Scheduling a Compliance Check”):

1. From the settings menu, select **Configuration**.
2. Click the **Settings** accordion, and select **Schedules**.
3. Click (**Configuration**), (**Add a new Schedule**).
4. In the **Adding a new Schedule** area, type in a name and description for the schedule.



5. Select **Active** if you want to enable this scan.
6. From the **Action** dropdown, select **Container Image Analysis**.
7. From the **Filter** dropdown, select **All Container Images for Containers Provider**, a new dropdown will appear. From this dropdown, choose the provider where you enabled the OpenSCAP policy profile.
8. From the **Run** dropdown, select how often you want the analysis to run. Your options after that depend on which run option you choose.



- 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.

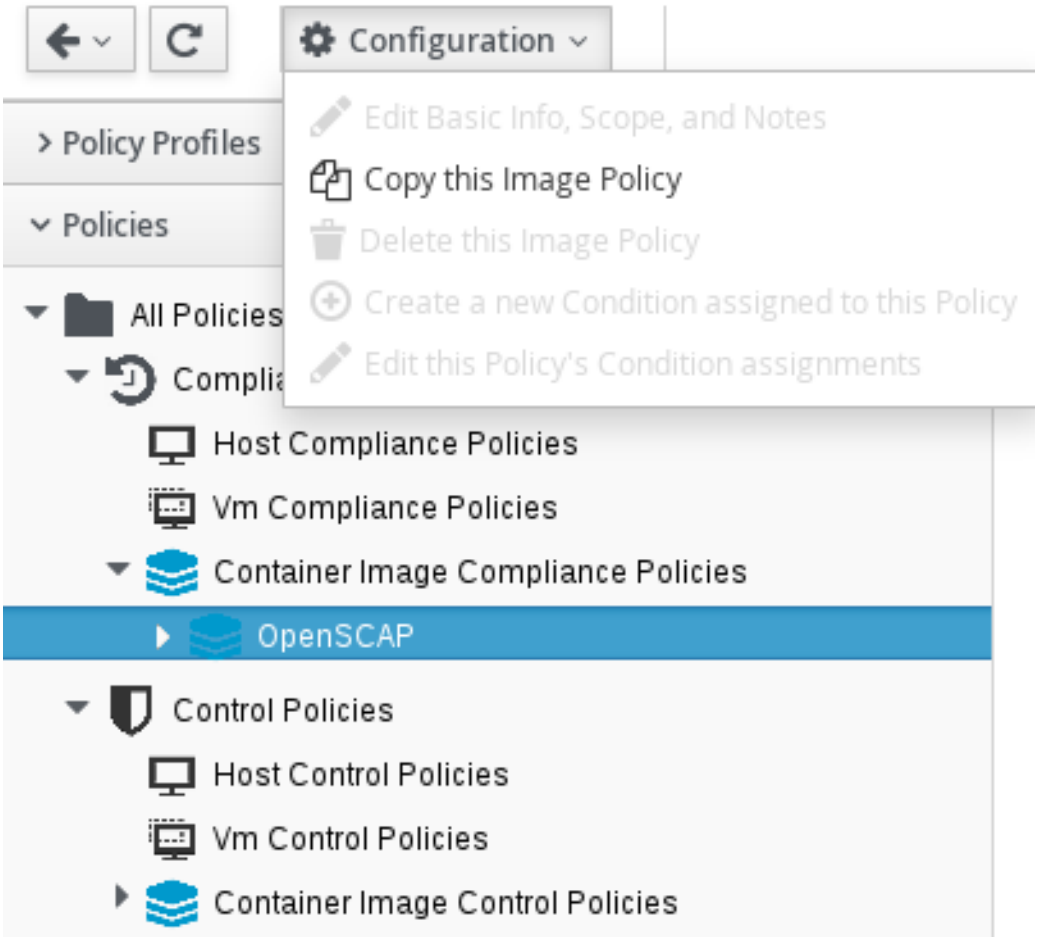
9. Select the time zone for the schedule.
10. Type or select a date to begin the schedule in **Starting Date**.
11. Select a starting time based on a 24-hour clock in the selected time zone.
12. Click **Add**.

A.3. CREATING A CUSTOMIZED OPENSCAP POLICY PROFILE

The built-in OpenSCAP policy profile cannot be edited. You can, however, assign *edited* copies of its policies to a new policy profile. This will allow you to create a *customized* version of the built-in OpenSCAP policy profile.

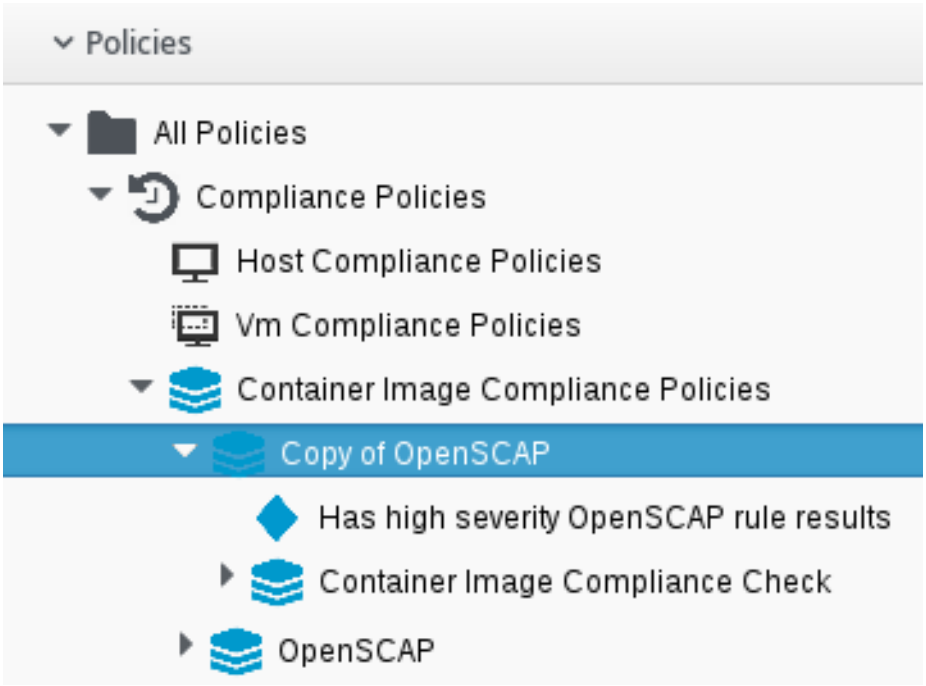
To do so, you will first have to copy the policy you want to customize:

1. Navigate to **Control** → **Explorer**.
2. Click the **Policies** accordion, and select the policy you want to copy.
3. Click  (**Configuration**), and an option to copy the policy should appear; for example,  (**Copy this Image Policy**).



4. Click **OK** to confirm.

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



You can now edit the copied policy. For instructions on how to edit policies, see:

- Section 1.1.2, “Editing Basic Information, Scope, and Notes for a Policy”

- Section 1.1.6, “Editing Policy Condition Assignments”
- Section 1.1.7, “Editing Policy Event Assignments”

After editing copied policies, you can now add them to a new policy profile. For instructions on how to create a new policy profile (and add policies to it), see Section 4.1, “Creating Policy Profiles” .

Once you have a customized policy profile, you can assign it to a container provider. See Section 4.4, “Assigning Policy Profiles” for instructions.