

# vRealize Operations Manager Configuration Guide

vRealize Operations Manager 6.5



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

About Configuration	6
<b>1 Connecting to Data Sources</b>	<b>7</b>
VMware vSphere Solution	7
Configure a vCenter Adapter Instance	9
Configure User Access for Actions	10
Endpoint Operations Management Solution	11
Endpoint Operations Management Agent Installation and Deployment	11
Roles and Privileges	53
Registering Agents on Clusters	53
Manually Create Operating System Objects	54
Managing Objects with Missing Configuration Parameters	55
Mapping Virtual Machines to Operating Systems	56
Customizing How Endpoint Operations Management Monitors Operating Systems	56
Log Insight	67
Log Insight Page	67
Logs Tab	68
Configuring vRealize Log Insight with vRealize Operations Manager	68
Business Management	69
Configure vRealize Business for Cloud Adapter	70
Installing Optional Solutions	71
Managing Solution Credentials	71
Managing Collector Groups	72
<b>2 Configuring Alerts and Actions</b>	<b>74</b>
Types of Alerts	74
Configuring Alerts	74
Defining Alerts in vRealize Operations Manager	74
Defining Symptoms for Alerts	75
Defining Recommendations for Alert Definitions	79
Create a New Alert Definition	79
Alert Definition Best Practices	81
Creating and Managing Alert Notifications	82
Create an Alert Definition for Department Objects	95
Alerts Group	106
Viewing Actions	107
List of vRealize Operations Manager Actions	108
Actions Supported for Automation	109

- [Integration of Actions with vRealize Automation](#) 111
- [Working With Actions That Use Power Off Allowed](#) 112

### **3 Configuring Policies** 116

- [Policies](#) 116
  - [Policy Decisions and Objectives](#) 118
  - [Policy Library Tab for Policies](#) 119
  - [Active Policies Tab for Policies](#) 121
- [Operational Policies](#) 124
  - [User Scenario: Create an Operational Policy for Production vCenter Server Datastore Objects](#) 125
- [Types of Policies](#) 135
  - [Custom Policies](#) 135
  - [Default Policy in vRealize Operations Manager](#) 144
  - [Policies Provided with vRealize Operations Manager](#) 145
- [Using the Monitoring Policy Workspace to Create and Modify Operational Policies](#) 146
  - [Policy Workspace in vRealize Operations Manager](#) 148

### **4 Configuring Super Metrics** 171

- [Create a Super Metric](#) 172
- [Enhancing Your Super Metrics](#) 175
- [Exporting and Importing a Super Metric](#) 176

### **5 Configuring Objects** 178

- [Object Discovery](#) 178
  - [About Objects](#) 179
  - [Managing Objects in Your Environment](#) 181
  - [Managing Custom Object Groups](#) 186
  - [Managing Application Groups](#) 190

### **6 Configuring Data Display** 192

- [Widgets](#) 192
  - [Widget Interactions](#) 193
  - [Manage Metric Configuration](#) 193
  - [Add a Resource Interaction XML File](#) 194
  - [Widget Definitions List](#) 195
- [Dashboards](#) 198
  - [Types Of Dashboards](#) 198
  - [Create and Configure Dashboards](#) 207
  - [Managing Dashboards](#) 210
- [Views](#) 213
  - [Views Overview](#) 214

Views and Reports Ownership	214
Create and Configure a View	214
Editing, Cloning, and Deleting a View	225
User Scenario: Create, Run, Export, and Import a vRealize Operations Manager View for Tracking Virtual Machines	226
Reports	228
Report Templates Tab	229
Generated Reports Tab	229
Create and Modify a Report Template	230
Add a Network Share Plug-In for vRealize Operations Manager Reports	233
User Scenario: Handling Reports to Monitor Virtual Machines	234
<b>7 Configuring Administration Settings</b>	<b>239</b>
Managing Users and Access Control	239
Users of vRealize Operations Manager	240
Roles and Privileges	244
User Scenario: Manage User Access Control	244
Configure a Single Sign-On Source	248
Audit Users and the Environment	251
Passwords and Certificates	252
Change the Administrator Password	252
Generate a Passphrase	253
Custom Certificates	253
Modifying Global Settings	257
List of Global Settings	257
Global Settings	259
Create a Support Bundle	260
Customizing Icons	261
Customize an Object Type Icon	261
Customize an Adapter Type Icon	262
<b>8 OPS-CLI Command-Line Tool</b>	<b>263</b>
dashboard Command Operations	264
template Command Operations	265
supermetric Command Operations	266
attribute Command Operations	267
reskind Command Operations for Object Types	267
report Command Operations	267
view Command Operations	267
file Command Operations	268

# About Configuration

The VMware *vRealize Operations Manager Configuration Guide* describes how to configure and monitor your environment. It shows you how to connect vRealize Operations Manager to external data sources and analyze the data collected from them, ensure that users and their supporting infrastructure are in place, configure resources to determine the behavior of your objects, and format the content that appears in vRealize Operations Manager.

To help you maintain and expand your vRealize Operations Manager installation, this information describes how to manage nodes and clusters, configure NTP, view log files, create support bundles, and add a maintenance schedule. It provides information about license keys and groups, and shows you how to generate a passphrase, review the certificates used for authentication, run the describe process, and perform advanced maintenance functions.

## Intended Audience

This information is intended for vRealize Operations Manager administrators, virtual infrastructure administrators, and operations engineers who install, configure, monitor, manage, and maintain the objects in your environment.

## VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

# Connecting vRealize Operations Manager to Data Sources

# 1

Configure solutions in vRealize Operations Manager to connect to and analyze data from external data sources in your environment. Once connected, you use vRealize Operations Manager to monitor and manage objects in your environment.

A solution might be only a connection to a data source, or it might include predefined dashboards, widgets, alerts, and views.

vRealize Operations Manager includes the VMware vSphere and Endpoint Operations Management solutions. These solutions are installed when you install vRealize Operations Manager.

Other solutions can be added to vRealize Operations Manager as management packs, such as the VMware Management Pack for NSX for vSphere. To download VMware management packs and other third-party solutions, visit the [VMware Solution Exchange](#).

This chapter includes the following topics:

- [VMware vSphere Solution in vRealize Operations Manager](#)
- [Endpoint Operations Management Solution in vRealize Operations Manager](#)
- [Log Insight](#)
- [Business Management](#)
- [Installing Optional Solutions in vRealize Operations Manager](#)

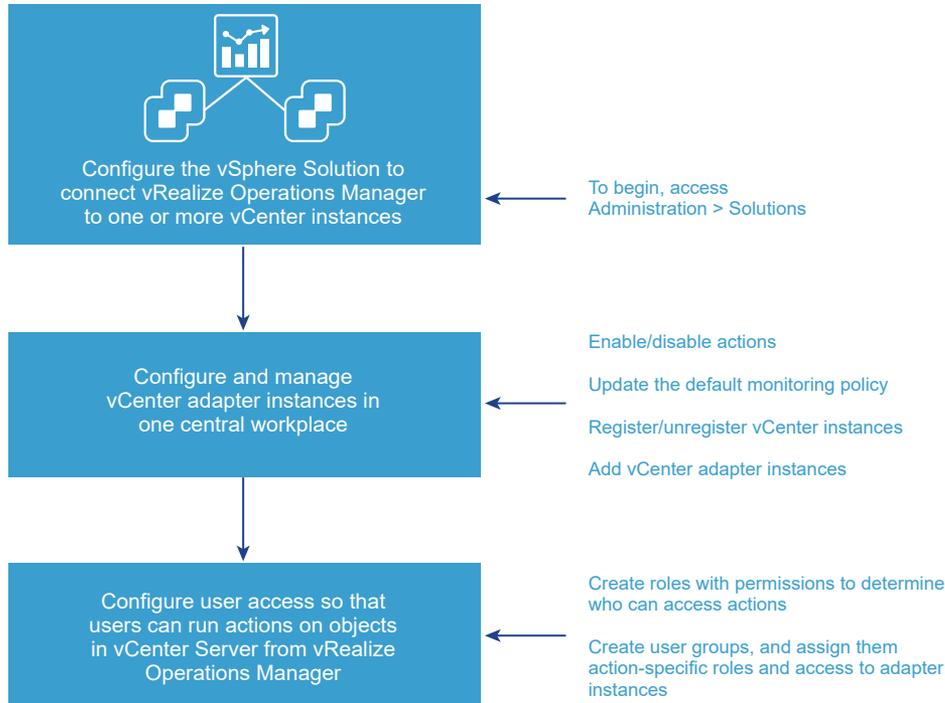
## VMware vSphere Solution in vRealize Operations Manager

The VMware vSphere solution connects vRealize Operations Manager to one or more vCenter Server instances. You collect data and metrics from those instances, monitor them, and run actions in them.

vRealize Operations Manager evaluates the data in your environment, identifying trends in object behavior, calculating possible problems and future capacity for objects in your system based on those trends, and alerting you when an object exhibits defined symptoms.

### Configuring the vSphere Solution

The vSphere solution is installed together with vRealize Operations Manager. The solution provides the vCenter Server adapter which you must configure to connect vRealize Operations Manager to your vCenter Server instances.



## How Adapter Credentials Work

The vCenter Server credentials that you use to connect vRealize Operations Manager to a vCenter Server instance, determines what objects vRealize Operations Manager monitors. Understand how these adapter credentials and user privileges interact to ensure that you configure adapters and users correctly, and to avoid some of the following issues.

- If you configure the adapter to connect to a vCenter Server instance with credentials that have permission to access only one of your three hosts, every user who logs in to vRealize Operations Manager sees only the one host, even when an individual user has privileges on all three of the hosts in the vCenter Server.
- If the provided credentials have limited access to objects in the vCenter Server, even vRealize Operations Manager administrative users can run actions only on the objects for which the vCenter Server credentials have permission.
- If the provided credentials have access to all the objects in the vCenter Server, any vRealize Operations Manager user who runs actions is using this account.

## Controlling User Access to Actions

Use the vCenter Server adapter to run actions on the vCenter Server from vRealize Operations Manager. If you choose to run actions, you must control user access to the objects in your vCenter Server environment. You control user access for local users based on how you configure user privileges in vRealize Operations Manager. If users log in using their vCenter Server account, then the way their account is configured in vCenter Server determines their privileges.

For example, you might have a vCenter Server user with a read-only role in vCenter Server. If you give this user the vRealize Operations Manager Power User role in vCenter Server rather than a more restrictive role, the user can run actions on objects because the adapter is configured with credentials that has privileges to change objects. To avoid this type of unexpected result, configure local vRealize Operations Manager users and vCenter Server users with the privileges you want them to have in your environment.

## Configure a vCenter Adapter Instance in vRealize Operations Manager

To manage your vCenter Server instances in vRealize Operations Manager, you must configure an adapter instance for each vCenter Server instance. The adapter requires the credentials that are used for communication with the target vCenter Server.

---

**Caution** Any adapter credentials you add are shared with other adapter administrators and vRealize Operations Manager collector hosts. Other administrators might use these credentials to configure a new adapter instance or to move an adapter instance to a new host.

---



Configure the vSphere Solution

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_config\\_vsphere\\_solution](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_config_vsphere_solution))

### Prerequisites

Verify that you know the vCenter Server credentials that have sufficient privileges to connect and collect data. If the provided credentials have limited access to objects in vCenter Server, all users, regardless of their vCenter Server privileges see only the objects that the provided credentials can access. At a minimum, the user account must have Read privileges and the Read privileges must be assigned at the data center or vCenter Server level.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon and click **Solutions**.
- 2 On the **Solutions** tab, select **VMware vSphere** and click the **Configure** button on the toolbar.
- 3 Enter a display name and description for the adapter instance.
- 4 In the **vCenter Server** text box, enter the FQDN or IP address of the vCenter Server instance to which you are connecting.

The vCenter Server FQDN or IP address must be reachable from all nodes in the vRealize Operations Manager cluster.

- 5 To add credentials for the vCenter Server instance, click the **Add** icon, and enter the required credentials.

- 6 The adapter is configured to run actions on objects in the vCenter Server from vRealize Operations Manager. If you do not want to run actions, select **Disable**.

The credentials provided for the vCenter Server instance are also used to run actions. If you do not want to use these credentials, you can provide alternative credentials by expanding **Alternate Action Credentials**, and clicking the **Add** icon.

- 7 Click **Test Connection** to validate the connection with your vCenter Server instance.
- 8 In the **Review and Accept Certificate** dialog box, review the certificate information.
- ◆ If the certificate presented in the dialog box matches the certificate for your target vCenter Server, click **OK**.
  - ◆ If you do not recognize the certificate as valid, click **Cancel**. The test fails and the connection to vCenter Server is not completed. You must provide a valid vCenter Server URL or verify the certificate on the vCenter Server is valid before completing the adapter configuration.
- 9 To modify the advanced options regarding collectors, object discovery, or change events, expand the **Advanced Settings**.

For information about these advanced settings, see the [#unique\\_5](#).

- 10 To adjust the default monitoring policy that vRealize Operations Manager uses to analyze and display information about the objects in your environment, click **Define Monitoring Goals**.

For information about the Define Monitoring Goals settings, see the [#unique\\_5](#).

- 11 To manage the registration of vCenter instances, click **Manage Registration**.

You can provide alternative credentials, or select the **Use collection credentials** check box to use the credentials specified when configuring this vCenter Server adapter instance.

- 12 Click **Save Settings**.

The adapter instance is added to the list.

vRealize Operations Manager begins collecting data from the vCenter Server instance. Depending on the number of managed objects, the initial collection can take more than one collection cycle. A standard collection cycle begins every five minutes.

### What to do next

If you configured the adapter to run actions, configure user access for the actions by creating action roles and user groups.

## Configure User Access for Actions

To ensure that users can run actions in vRealize Operations Manager, you must configure user access to the actions.

You use role permissions to control who can run actions. You can create multiple roles. Each role can give users permissions to run different subsets of actions. Users who hold the Administrator role or the default super user role already have the required permissions to run actions.

You can create user groups to add action-specific roles to a group rather than configuring individual user privileges.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click **Administration > Access Control**.
- 2 To create a role:
  - a Click the **Roles** tab.
  - b Click the **Add** icon, and enter a name and description for the role.
- 3 To apply permissions to the role, select the role, and in the Permissions pane, click the **Edit** icon.
  - a Expand **Environment**, and then expand **Action**.
  - b Select one or more of the actions, and click **Update**.
- 4 To create a user group:
  - a Click the **User Groups** tab, and click the **Add** icon.
  - b Enter a name for the group and a description, and click **Next**.
  - c Assign users to the group, and click the **Objects** tab.
  - d Select a role that has been created with permissions to run actions, and select the **Assign this role to the user** check box.
  - e Configure the object privileges by selecting each adapter instance to which the group needs access to run actions.
  - f Click **Finish**.

### What to do next

Test the users that you assigned to the group. Log out, and log back in as one of the users. Verify that this user can run the expected actions on the selected adapter.

## Endpoint Operations Management Solution in vRealize Operations Manager

You configure Endpoint Operations Management to gather operating system metrics and to monitor availability of remote platforms and applications. This solution is installed with vRealize Operations Manager.

## Endpoint Operations Management Agent Installation and Deployment

Use the information in these links to help you to install and deploy Endpoint Operations Management agents in your environment.

## Prepare to Install the Endpoint Operations Management Agent

Before you can install the Endpoint Operations Management agent, you must perform preparatory tasks.

### Prerequisites

- To configure the agent to use a keystore that you manage yourself for SSL communication, set up a JKS-format keystore for the agent on its host and import its SSL certificate. Make a note of the full path to the keystore, and its password. You must specify this data in the agent's `agent.properties` file.

Verify that the agent keystore password and the private key password are identical.

- Define the agent `HQ_JAVA_HOME` location.

vRealize Operations Manager platform-specific installers include JRE 1.8.x. Depending on your environment and the installer you use, you may need to define the location of the JRE to ensure that the agent can find the JRE to use. See [Configuring JRE Locations for Endpoint Operations Management Components](#).

## Supported Operating Systems for the Endpoint Operations Management Agent

These tables describe the supported operating systems for Endpoint Operations Management agent deployments.

These configurations are supported for the agent in both development and production environments.

**Table 1-1. Supported Operating Systems for the Endpoint Operations Management Agent**

Operating System	Processor Architecture	JVM
RedHat Enterprise Linux (RHEL) 5.x, 6.x, 7.x	x86_64, x86_32	Oracle Java SE8
CentOS 5.x, 6.x, 7.x	x86_64, x86_32	Oracle Java SE8
SUSE Enterprise Linux (SLES) 11.x, 12.x	x86_64	Oracle Java SE8
Windows 2008 Server, 2008 Server R2	x86_64, x86_32	Oracle Java SE8
Windows 2012 Server, 2012 Server R2	x86_64	Oracle Java SE8
Solaris 10, 11	x86_64, SPARC	Oracle Java SE7
AIX 6.1, 7.1	Power PC	IBM Java SE7
VMware Photon Linux 1.0	x86_64	Open JDK 1.8.0_72-BLFS
Oracle Linux versions 5, 6, 7	x86_64, x86_32	Open JDK Runtime Environment 1.7

## Selecting an Agent Installer Package

The Endpoint Operations Management agent installation files are included in the vRealize Operations Manager installation package.

You can install the Endpoint Operations Management agent from a `tar.gz` or `.zip` archive, or from an operating system-specific installer for Windows or for Linux-like systems that support RPM.

Note that when you install a non-JRE version of Endpoint Operations Management agent, to avoid being exposed to security risks related to earlier versions of Java, VMware recommends that you only use the latest Java version.

- [Install the Agent on a Linux Platform from an RPM Package](#)

You can install the Endpoint Operations Management agent from a RedHat Package Manager (RPM) package. The agent in the `noarch` package does not include a JRE.

- [Install the Agent on a Linux Platform from an Archive](#)

You can install an Endpoint Operations Management agent on a Linux platform from a `tar.gz` archive.

- [Install the Agent on a Windows Platform from an Archive](#)

You can install an Endpoint Operations Management agent on a Windows platform from a `.zip` file.

- [Install the Agent on a Windows Platform Using the Windows Installer](#)

You can install the Endpoint Operations Management agent on a Windows platform using a Windows installer.

- [Installing an Endpoint Operations Management Agent Silently on a Windows Machine](#)

You can install an Endpoint Operations Management agent on a Windows machine using silent or very silent installation.

### Install the Agent on a Linux Platform from an RPM Package

You can install the Endpoint Operations Management agent from a RedHat Package Manager (RPM) package. The agent in the `noarch` package does not include a JRE.

Agent-only archives are useful when you deploy agents to a large number of platforms with various operating systems and architectures. Agent archives are available for Windows and UNIX-like environments, with and without built-in JREs.

The RPM performs the following actions:

- Creates a user and group named `epops` if they do not exist. The user is a service account that is locked and you cannot log into it.
- Installs the agent files into `/opt/vmware/epops-agent`.
- Installs an init script to `/etc/init.d/epops-agent`.
- Adds the `init` script to `chkconfig` and sets it to on for run levels 2, 3, 4, and 5.

If you have multiple agents to install, see [Install Multiple Endpoint Operations Management Agents Simultaneously](#).

### Prerequisites

- Verify that you have sufficient privileges to deploy an Endpoint Operations Management agent. You must have vRealize Operations Manager user credentials that include a role that allows you to install Endpoint Operations Management agents. See [Roles and Privileges in vRealize Operations Manager](#).

- If you plan to run ICMP checks, you must install the Endpoint Operations Management agent with **root** privileges.
- To configure the agent to use a keystore that you manage yourself for SSL communication, set up a JKS-format keystore for the agent on its host and configure the agent to use its SSL certificate. Note the full path to the keystore, and its password. You must specify this data in the agent `agent.properties` file.

Verify that the agent keystore password and the private key password are identical.

- If you are installing a non-JRE package, define the agent `HQ_JAVA_HOME` location.  
Endpoint Operations Management platform-specific installers include JRE 1.8.x. Platform-independent installers do not. Depending on your environment and the installer you use, you might need to define the location of the JRE to ensure that the agent can find the JRE to use. See [Configuring JRE Locations for Endpoint Operations Management Components](#).
- If you are installing a non-JRE package, verify that you are using the latest Java version. You might be exposed to security risks with earlier versions of Java.
- Verify that the installation directory for the Endpoint Operations Management agent does not contain a vRealize Hyperic agent installation.
- If you are using the noarch installation, verify that a JDK or JRE is installed on the platform.
- Verify that you use only ASCII characters when specifying the agent installation path. If you want to use non-ASCII characters, you must set the encoding of the Linux machine and SSH client application to UTF-8.

## Procedure

- 1 Download the appropriate RPM bundle to the target machine.

Operating System	RPM Bundle to Download
64bit Operating System	<code>epops-agent-x86-64-linux-version.rpm</code>
32bit Operating System	<code>epops-agent-x86-linux-version.rpm</code>
No Arch	<code>epops-agent-noarch-linux-version.rpm</code>

- 2 Open an SSH connection using `root` credentials.
- 3 Run `rpm -i epops-agent-Arch-linux-version.rpm` to install the agent on the platform that the agent will monitor, where *Arch* is the name of the archive and *version* is the version number.

The Endpoint Operations Management agent is installed, and the service is configured to start at boot.

## What to do next

Before you start the service, verify that the `epops` user credentials include any permissions that are required to enable your plug-ins to discover and monitor their applications, then perform one of the following processes.

- Run `service epops-agent start` to start the `epops-agent` service.

- If you installed the Endpoint Operations Management agent on a machine running SuSE 12.x, start the Endpoint Operations Management agent by running the `[EP_Ops_Home]/bin/ep-agent.sh` start command.
- When you attempt to start an Endpoint Operations Management agent you might receive a message that the agent is already running. Run `./bin/ep-agent.sh stop` before starting the agent.
- Configure the agent in the `agent.properties` file, then start the service. See [Activate Endpoint Operations Management Agent to vRealize Operations Manager Server Setup Properties](#).

### Install the Agent on a Linux Platform from an Archive

You can install an Endpoint Operations Management agent on a Linux platform from a `tar.gz` archive.

By default, during installation, the setup process prompts you to provide configuration values. You can automate this process by specifying the values in the agent properties file. If the installer detects values in the properties file, it applies those values. Subsequent deployments also use the values specified in the agent properties file.

#### Prerequisites

- Verify that you have sufficient privileges to deploy an Endpoint Operations Management agent. You must have vRealize Operations Manager user credentials that include a role that allows you to install Endpoint Operations Management agents. See [Roles and Privileges in vRealize Operations Manager](#).
- If you plan to run ICMP checks, you must install the Endpoint Operations Management agent with **root** privileges.
- Verify that the installation directory for the Endpoint Operations Management agent does not contain a vRealize Hyperic agent installation.
- Verify that you use only ASCII characters when specifying the agent installation path. If you want to use non-ASCII characters, you must set the encoding of the Linux machine and SSH client application to UTF-8.

#### Procedure

- 1 Download and extract the Endpoint Operations Management agent installation `tar.gz` file that is appropriate for your Linux operating system.

Operating System	tar.gz Bundle to Download
64bit Operating System	<code>epops-agent-x86-64-linux-version.tar.gz</code>
32bit Operating System	<code>epops-agent-x86-linux-version.tar.gz</code>
No Arch	<code>epops-agent-noJRE-version.tar.gz</code>

- 2 Run `cd agent_name/bin` to open the `bin` directory for the agent.

### 3 Run `ep-agent.sh start`.

The first time that you install the agent, the command launches the setup process, unless you already specified all the required configuration values in the agent properties file.

### 4 (Optional) Run `ep-agent.sh status` to view the current status of the agent, including the IP address and port.

#### What to do next

Register the client certificate for the agent. See [Regenerate an Agent Client Certificate](#).

#### Install the Agent on a Windows Platform from an Archive

You can install an Endpoint Operations Management agent on a Windows platform from a .zip file.

By default, during installation, the setup process prompts you to provide configuration values. You can automate this process by specifying the values in the agent properties file. If the installer detects values in the properties file, it applies those values. Subsequent deployments also use the values specified in the agent properties file.

#### Prerequisites

- Verify that you have sufficient privileges to deploy a Endpoint Operations Management agent. You must have vRealize Operations Manager user credentials that include a role that allows you to install Endpoint Operations Management agents. See [Roles and Privileges in vRealize Operations Manager](#).
- Verify that the installation directory for the Endpoint Operations Management agent does not contain a vRealize Hyperic agent installation.
- Verify that you do not have any Endpoint Operations Management or vRealize Hyperic agent installed on your environment before running the agent Windows installer.

#### Procedure

- 1 Download and extract the Endpoint Operations Management agent installation .zip file that is appropriate for your Windows operating system.

Operating System	ZIP Bundle to Download
64bit Operating System	<code>epops-agent-x86-64-win-version.zip</code>
32bit Operating System	<code>epops-agent-win32-version.zip</code>
No Arch	<code>epops-agent-noJRE-version.zip</code>

- 2 Run `cd agent_name\bin` to open the bin directory for the agent.
- 3 Run `ep-agent.bat install`.
- 4 Run `ep-agent.bat start`.

The first time that you install the agent, the command starts the setup process, unless you already specified the configuration values in the agent properties file.

**What to do next**

Generate the client certificate for the agent. See [Regenerate an Agent Client Certificate](#).

**Install the Agent on a Windows Platform Using the Windows Installer**

You can install the Endpoint Operations Management agent on a Windows platform using a Windows installer.

You can perform a silent installation of the agent. See [Installing an Endpoint Operations Management Agent Silently on a Windows Machine](#).

**Prerequisites**

- Verify that you have sufficient privileges to deploy an Endpoint Operations Management agent. You must have vRealize Operations Manager user credentials that include a role that allows you to install Endpoint Operations Management agents. See [Roles and Privileges in vRealize Operations Manager](#).
- Verify that the installation directory for the Endpoint Operations Management agent does not contain a vRealize Hyperic agent installation.
- If you already have an Endpoint Operations Management agent installed on the machine, verify that it is not running.
- Verify that you do not have any Endpoint Operations Management or vRealize Hyperic agent installed on your environment before running the agent Windows installer.
- You must know the user name and password for the vRealize Operations Manager, the vRealize Operations Manager server address (FQDN), and the server certificate thumbprint value. You can see additional information about the certificate thumbprint in the procedure.

**Procedure**

- 1 Download the Windows installation EXE file that is appropriate for your Windows platform.

Operating System	RPM Bundle to Download
64bit Operating System	<code>epops-agent-x86-64-win-version.exe</code>
32bit Operating System	<code>epops-agent-x86-win-version.exe</code>

- 2 Double-click the file to open the installation wizard.
- 3 Complete the steps in the installation wizard.

Verify that the user and system locales are identical, and that the installation path contains only characters that are part of the system locale's code page. You can set user and system locales in the Regional Options or Regional Settings control panel.

Note the following information related to defining the server certificate thumbprint.

- The server certificate thumbprint is required to run a silent installation.
- Either the SHA1 or SHA256 algorithm can be used for the thumbprint.

- By default, the vRealize Operations Manager server generates a self-signed CA certificate that is used to sign the certificate of all the nodes in the cluster. In this case, the thumbprint must be the thumbprint of the CA certificate, to allow for the agent to communicate with all nodes.
- As a vRealize Operations Manager administrator, you can import a custom certificate instead of using the default. In this instance, you must specify a thumbprint corresponding to that certificate as the value of this property.
- To view the certificate thumbprint value, log into the vRealize Operations Manager Administration interface at `https://IP Address/admin` and click the **SSL Certificate** icon located on the right of the menu bar. Unless you replaced the original certificate with a custom certificate, the second thumbprint in the list is the correct one. If you did upload a custom certificate, the first thumbprint in the list is the correct one.

#### 4 (Optional) Run `ep-agent.bat query` to verify if the agent is installed and running.

The agent begins running on the Windows platform.

---

**Caution** The agent will run even if some of the parameters that you provided in the installation wizard are missing or invalid. Check the `wrapper.log` and `agent.log` files in the *product installation path*/Log directory to verify that there are no installation errors.

---

### Installing an Endpoint Operations Management Agent Silently on a Windows Machine

You can install an Endpoint Operations Management agent on a Windows machine using silent or very silent installation.

Silent and very silent installations are performed from a command line interface using a setup installer executable file.

Verify that you do not have any Endpoint Operations Management or vRealize Hyperic agent installed on your environment before running the agent Windows installer.

Use the following parameters to set up the installation process. For more information about these parameters, see [Specify the Endpoint Operations Management Agent Setup Properties](#).

---

**Caution** The parameters that you specify for the Windows installer are passed to the agent configuration without validation. If you provide an incorrect IP address or user credentials, the Endpoint Operations Management agent cannot start.

---

**Table 1-2. Silent Command Line Installer Parameters**

Parameter	Value	Mandatory/ Optional	Comments
<code>-serverAddress</code>	FQDN/IP address	Mandatory	FQDN or IP address of the vRealize Operations Manager server.
<code>-username</code>	string	Mandatory	
<code>-securePort</code>	number	Optional	Default is 443

Parameter	Value	Mandatory/ Optional	Comments
-password	string	Mandatory	
-serverCertificateThumbprint	string	Mandatory	The vRealize Operations Manager server certificate thumbprint. You must enclose the certificate thumbprint in opening and closing quotation marks, for example, -serverCertificateThumbprint "31:32:FA:1F:FD:78:1E:D8:9A:15:32:85:D7:FE:54:49:0A:1D:9F:6D" .

Parameters are available to define various other attributes for the installation process.

**Table 1-3. Additional Silent Command Line Installer Parameters**

Parameter	Default Value	Comments
/DIR	C:\ep-agent	Specifies the installation path. You cannot use spaces in the installation path, and you must connect the /DIR command and the installation path with an equal sign, for example, /DIR=C:\ep-agent.
/SILENT	none	Specifies that the installation is to be silent. In a silent installation, only the progress window appears.
/VERYSILENT	none	Specifies that the installation is to be very silent. In a very silent installation, the progress window does not appear, however installation error messages are displayed, as is the startup prompt if you did not disable it.

## Java Prerequisites for the Endpoint Operations Management Agent

All Endpoint Operations Management agents require Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction policy files be included as part of the Java package.

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction policy files are included in the JRE Endpoint Operations Management agent installation options.

You can install an Endpoint Operations Management agent package that does not contain JRE files, or choose to add JRE later.

If you select a non-JRE installation option, you must ensure that your Java package includes Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction policy files to enable registration of the Endpoint Operations Management agent. If you select a non-JRE option and your Java package does not include Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction policy files, you receive these error messages Server might be down (or wrong IP/port were used) and Cannot support TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA with currently installed providers.

## Configuring JRE Locations for Endpoint Operations Management Components

Endpoint Operations Management agents require a JRE. The platform-specific Endpoint Operations Management agent installers include a JRE. Platform-independent Endpoint Operations Management agent installers do not include a JRE.

If you select a non-JRE installation option, you must ensure that your Java package includes Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction policy files to enable registration of the Endpoint Operations Management agent. For more information, see [Java Prerequisites for the Endpoint Operations Management Agent](#).

Depending on your environment and the installation package that you use, you might need to define the location of the JRE for your agents. The following environments require JRE location configuration.

- Platform-specific agent installation on a machine that has its own JRE that you want to use
- Platform-independent agent installation

### How the Agent Resolves its JRE

The agent resolves its JRE based on platform type.

**UNIX-like Platforms**      On UNIX-like platforms, the agent determines which JRE to use in the following order:

- 1    HQ\_JAVA\_HOME environment variable
- 2    Embedded JRE
- 3    JAVA\_HOME environment variable

**Linux Platforms**      On Linux platforms, you use `export HQ_JAVA_HOME=path_to_current_java_directory` to define a system variable.

**Windows Platforms**      On Windows platforms, the agent resolves the JRE to use in the following order:

- 1    HQ\_JAVA\_HOME environment variable

The path defined in the variable must not contain spaces. Consider using a shortened version of the path, using the tild (~) character. For example, `c:\Program Files\Java\jre7` can become `c:\Progra~1\Java\jre7`. The number after the tild depends on the alphabetical order (where a = 1, b =2, and so on) of files whose name begins with `progra` in that directory.

- 2    Embedded JRE

You define a system variable from the **My Computer** menu. Select **Properties > Advanced > Environment Variables > System Variables > New**.

Because of a known issue with Windows, on Windows Server 2008 R2 and 2012 R2, Windows services might keep old values of system variables, even though they have been updated or removed. As a result, updates or removal of the `HQ_JAVA_HOME` system variable might not be propagated to the Endpoint Operations Management Agent service. In this event, the Endpoint Operations Management agent might use an obsolete value for `HQ_JAVA_HOME`, which will cause it to use the wrong JRE version.

## System Prerequisites for the Endpoint Operations Management Agent

If you do not define `localhost` as the loopback address, the Endpoint Operations Management agent does not register and the following error appears: `Connection failed. Server may be down (or wrong IP/port were used). Waiting for 10 seconds before retrying.`

As a workaround, complete the following steps:

### Procedure

- 1 Open the hosts file `/etc/hosts` on Linux or `C:\Windows\System32\Drivers\etc\hosts` on Windows.
- 2 Modify the file to include a `localhost` mapping to the IPv4 `127.0.0.1` loopback address, using `127.0.0.1 localhost`.
- 3 Save the file.

Endpoint Operations Management agent does not support IPv6.

## Configure the Endpoint Operations Management Agent to vRealize Operations Manager Server Communication Properties

Before first agent startup, you can define the properties that enable the agent to communicate with the vRealize Operations Manager server, and other agent properties, in the `agent.properties` file of an agent. When you configure the agent in the properties file you can streamline the deployment for multiple agents.

If a properties file exists, back it up before you make configuration changes. If the agent does not have a properties file, create one.

An agent looks for its properties file in `AgentHome/conf`. This is the default location of `agent.properties`.

If the agent does not find the required properties for establishing communications with the vRealize Operations Manager server in either of these locations, it prompts for the property values at initial start up of the agent.

A number of steps are required to complete the configuration.

You can define some agent properties before or after the initial startup. You must always configure properties that control the following behaviors before initial startup.

- When the agent must use an SSL keystore that you manage, rather than a keystore that vRealize Operations Manager generates.
- When the agent must connect to the vRealize Operations Manager server through a proxy server.

## Prerequisites

Verify that the vRealize Operations Manager server is running.

## Procedure

### 1 [Activate Endpoint Operations Management Agent to vRealize Operations Manager Server Setup Properties](#)

In the `agent.properties` file, properties relating to communication between the Endpoint Operations Management agent and the vRealize Operations Manager server are inactive by default. You must activate them.

### 2 [Specify the Endpoint Operations Management Agent Setup Properties](#)

The `agent.properties` file contains properties that you can configure to manage communication.

### 3 [Configure an Endpoint Operations Management Agent Keystore](#)

The agent uses a self-signed certificate for internal communication, and a second certificate that is signed by the server during the agent registration process. By default, the certificates are stored in a keystore that is generated in the `data` folder. You can configure your own keystore for the agent to use.

### 4 [Configure the Endpoint Operations Management Agent by Using the Configuration Dialog](#)

The Endpoint Operations Management agent configuration dialog appears in the shell when you start an agent that does not have configuration values that specify the location of the vRealize Operations Manager server. The dialog prompts you to provide the address and port of the vRealize Operations Manager server, and other connection-related data.

### 5 [Overriding Agent Configuration Properties](#)

You can specify that vRealize Operations Manager override default agent properties when they differ from custom properties that you have defined.

### 6 [Endpoint Operations Management Agent Properties](#)

Multiple properties are supported in the `agent.properties` file for an Endpoint Operations Management agent. Not all supported properties are included by default in the `agent.properties` file.

## What to do next

Start the Endpoint Operations Management agent.

## Activate Endpoint Operations Management Agent to vRealize Operations Manager Server Setup Properties

In the `agent.properties` file, properties relating to communication between the Endpoint Operations Management agent and the vRealize Operations Manager server are inactive by default. You must activate them.

## Procedure

- 1 In the `agent.properties` file, locate the following section.

```
## Use the following to automate agent setup
## using these properties.
##
## If any properties do not have values specified, the setup
## process prompts for their values.
##
## If the value to use during automatic setup is the default, use the string *default* as the
## value for the option.
```

- 2 Remove the hash tag at the beginning of each line to activate the properties.

```
#agent.setup.serverIP=localhost
#agent.setup.serverSSLPort=443
#agent.setup.serverLogin=username
#agent.setup.serverPword=password
```

The first time that you start the Endpoint Operations Management agent, if `agent.setup.serverPword` is inactive, and has a plain text value, the agent encrypts the value.

- 3 (Optional) Remove the hash tag at the beginning of the line `#agent.setup.serverCertificateThumbprint=` and provide a thumbprint value to activate pre-approval of the server certificate.

## Specify the Endpoint Operations Management Agent Setup Properties

The `agent.properties` file contains properties that you can configure to manage communication.

Agent-server setup requires a minimum set of properties.

### Procedure

- 1 Specify the location and credentials the agent must use to contact the vRealize Operations Manager server.

Property	Property Definition
<code>agent.setup.serverIP</code>	Specify the address or hostname of the vRealize Operations Manager server.
<code>agent.setup.serverSSLPort</code>	The default value is the standard SSL vRealize Operations Manager server listen port. If your server is configured for a different listen port, specify the port number.
<code>agent.setup.serverLogin</code>	Specify the user name for the agent to use when connecting to the vRealize Operations Managerserver. If you change the value from the <code>username</code> default value, verify that the user account is correctly configured on the vRealize Operations Manager server.
<code>agent.setup.serverPword</code>	Specify the password for the agent to use, together with the user name specified in <code>agent.setup.camLogin</code> , when connecting to the vRealize Operations Manager server. Verify that the password is the one configured in vRealize Operations Manager for the user account.

## 2 (Optional) Specify the vRealize Operations Manager server certificate thumbprint.

Property	Property Definition
<b>agent.setup.serverCertificateThumbprint</b>	<p>Provides details about the server certificate to trust.</p> <p>This parameter is required to run a silent installation.</p> <p>Either the SHA1 or SHA256 algorithm can be used for the thumbprint.</p> <p>By default, the vRealize Operations Manager server generates a self-signed CA certificate that is used to sign the certificate of all the nodes in the cluster. In this case, the thumbprint must be the thumbprint of the CA certificate, to allow for the agent to communicate with all nodes.</p> <p>As a vRealize Operations Manager administrator, you can import a custom certificate instead of using the default. In this instance, you must specify a thumbprint corresponding to that certificate as the value of this property.</p> <p>To view the certificate thumbprint value, log into the vRealize Operations Manager Administration interface at <a href="https://IP Address/admin">https://IP Address/admin</a> and click the <b>SSL Certificate</b> icon located on the right of the menu bar. Unless you replaced the original certificate with a custom certificate, the second thumbprint in the list is the correct one. If you did upload a custom certificate, the first thumbprint in the list is the correct one.</p>

## 3 (Optional) Specify the location and file name of the platform token file.

This file is created by the agent during installation and contains the identity token for the platform object.

Property	Property Definition
<b>Windows:</b> <b>agent.setup.tokenFileWindows</b> <b>Linux: agent.setup.tokenFileLinux</b>	<p>Provides details about the location and name of the platform token file.</p> <p>The value cannot include backslash (\) or percentage(%) characters, or environment variables.</p> <p>Ensure that you use forward slashes (/) when specifying the Windows path.</p>

## 4 (Optional) Specify any other required properties by running the appropriate command.

Operating System	Command
<b>Linux</b>	<code>./bin/ep-agent.sh set-property <i>PropertyKey</i> <i>PropertyValue</i></code>
<b>Windows</b>	<code>./bin/ep-agent.bat set-property <i>PropertyKey</i> <i>PropertyValue</i></code>

The properties are encrypted in the `agent.properties` file.

## Configure an Endpoint Operations Management Agent Keystore

The agent uses a self-signed certificate for internal communication, and a second certificate that is signed by the server during the agent registration process. By default, the certificates are stored in a keystore that is generated in the `data` folder. You can configure your own keystore for the agent to use.

**Important** To use your own keystore, you must perform this task before the first agent activation.

## Procedure

- 1 In the `agent.properties` file, activate the `# agent.keystore.path=` and `# agent.keystore.password=` properties.

Define the full path to the keystore with `agent.keystore.path` and the keystore password with `agent.keystore.password`.

- 2 Add the `[agent.keystore.alias]` property to the properties file, and set it to the alias of the primary certificate or private key entry of the keystore primary certificate.

## Configure the Endpoint Operations Management Agent by Using the Configuration Dialog

The Endpoint Operations Management agent configuration dialog appears in the shell when you start an agent that does not have configuration values that specify the location of the vRealize Operations Manager server. The dialog prompts you to provide the address and port of the vRealize Operations Manager server, and other connection-related data.

The agent configuration dialog appears in these cases:

- The first time that you start an agent, if you did not supply one or more of the relevant properties in the `agent.properties` file.
- When you start an agent for which saved server connection data is corrupt or was removed.

You can also run the agent launcher to rerun the configuration dialog.

## Prerequisites

Verify that the server is running.

## Procedure

- 1 Open a terminal window on the platform on which the agent is installed.
- 2 Navigate to the `AgentHome/bin` directory.
- 3 Run the agent launcher using the `start` or `setup` option.

Platform	Command
UNIX-like	<code>ep-agent.sh start</code>
Windows	<p>Install the Windows service for the agent, then run the <code>it: ep-agent.bat install ep-agent.bat start</code> command.</p> <p>When you configure an Endpoint Operations Management agent as a Windows service, make sure that the credentials that you specify are sufficient for the service to connect to the monitored technology. For example, if you have an Endpoint Operations Management agent that is running on Microsoft SQL Server, and only a specific user can log in to that server, the Windows service login must also be for that specific user.</p>

#### 4 Respond to the prompts, noting the following as you move through the process.

Prompt	Description
<b>Enter the server hostname or IP address</b>	If the server is on the same machine as the agent, you can enter <code>localhost</code> . If a firewall is blocking traffic from the agent to the server, specify the address of the firewall.
<b>Enter the server SSL port</b>	Specify the SSL port on the vRealize Operations Manager server to which the agent must connect. The default port is 443.
<b>The server has presented an untrusted certificate</b>	If this warning appears, but your server is signed by a trusted certificate or you have updated the <code>thumbprint</code> property to contain the thumbprint, this agent might be subject to a man-in-the-middle attack. Review the displayed certificate thumbprint details carefully.
<b>Enter your server username</b>	Enter the name of a vRealize Operations Manager user with <code>agentManager</code> permissions.
<b>Enter your server password</b>	Enter the password for the specified vRealize Operations Manager. Do not store the password in the <code>agent.properties</code> file.

The agent initiates a connection to the vRealize Operations Manager server and the server verifies that the agent is authenticated to communicate with it.

The server generates a client certificate that includes the agent token. The message `The agent has been successfully registered` appears. The agent starts discovering the platform and supported products running on it.

### Overriding Agent Configuration Properties

You can specify that vRealize Operations Manager override default agent properties when they differ from custom properties that you have defined.

In the Advanced section of the Edit Object dialog, if you set the **Override agent configuration data** to **false**, default agent configuration data is applied. If you set **Override agent configuration data** to **true**, the default agent parameter values are ignored if you have set alternative values, and the values that you set are applied.

If you set the value of **Override agent configuration data** to **true** when editing an MSSQL object (MSSQL, MSSQL Database, MSSQL Reporting Services, MSSQL Analysis Service, or MSSQL Agent) that runs in a cluster, it might result in inconsistent behavior.

### Endpoint Operations Management Agent Properties

Multiple properties are supported in the `agent.properties` file for an Endpoint Operations Management agent. Not all supported properties are included by default in the `agent.properties` file.

You must add any properties that you want to use that are not included in the default `agent.properties` file.

You can encrypt properties in the `agent.properties` file to enable silent installation.

#### Encrypt Endpoint Operations Management Agent Property Values

After you have installed an Endpoint Operations Management agent, you can use it to add encrypted values to the `agent.properties` file to enable silent installation.

For example, to specify the user password, you can run `./bin/ep-agent.sh set-property agent.setup.serverPword serverPasswordValue` to add the following line to the `agent.properties` file.

```
agent.setup.serverPword = ENC(4FyUf6m/c5i+RriaNpSEQ1WKGb4y
+Dhp7213XQiyvtwI4tMlbGJfZMBPG23KnsUWu30KrW35gB+Ms20snM4TDg==)
```

The key that was used to encrypt the value is saved in `AgentHome/conf/agent.scu`. If you encrypt other values, the key that was used to encrypt the first value is used.

### Prerequisites

Verify that the Endpoint Operations Management agent can access `AgentHome/conf/agent.scu`. Following the encryption of any agent-to-server connection properties, the agent must be able to access this file to start.

### Procedure

- ◆ Open a command prompt and run `./bin/ep-agent.sh set-property agent.setup.propertyName propertyValue`.

The key that was used to encrypt the value is saved in `AgentHome/conf/agent.scu`.

### What to do next

If your agent deployment strategy involves distributing a standard `agent.properties` file to all agents, you must also distribute `agent.scu`. See [Install Multiple Endpoint Operations Management Agents Simultaneously](#).

### Adding Properties to the agent.properties File

You must add any properties that you want to use that are not included in the default `agent.properties` file.

Following is a list of the available properties.

- [agent.keystore.alias Property](#)  
This property configures the name of the user-managed keystore for the agent for agents configured for unidirectional communication with the vRealize Operations Manager server.
- [agent.keystore.password Property](#)  
This property configures the password for an Endpoint Operations Management agent's SSL keystore.
- [agent.keystore.path Property](#)  
This property configures the location of a Endpoint Operations Management agent's SSL keystore.
- [agent.listenPort Property](#)  
This property specifies the port where the Endpoint Operations Management agent listens to receive communication from the vRealize Operations Manager server.

- [agent.logDir Property](#)

You can add this property to the `agent.properties` file to specify the directory where the Endpoint Operations Management agent writes its log file. If you do not specify a fully qualified path, `agent.logDir` is evaluated relative to the agent installation directory.

- [agent.logFile Property](#)

The path and name of the agent log file.

- [agent.logLevel Property](#)

The level of detail of the messages the agent writes to the log file.

- [agent.logLevel.SystemErr Property](#)

Redirects `System.err` to the `agent.log` file.

- [agent.logLevel.SystemOut Property](#)

Redirects `System.out` to the `agent.log` file.

- [agent.proxyHost Property](#)

The host name or IP address of the proxy server that the Endpoint Operations Management agent must connect to first when establishing a connection to the vRealize Operations Manager server.

- [agent.proxyPort Property](#)

The port number of the proxy server that the Endpoint Operations Management agent must connect to first when establishing a connection to the vRealize Operations Manager server.

- [agent.setup.acceptUnverifiedCertificate Property](#)

This property controls whether an Endpoint Operations Management agent issues a warning when the vRealize Operations Manager server presents an SSL certificate that is not in the agent's keystore, and is either self-signed or signed by a different certificate authority than the one that signed the agent's SSL certificate.

- [agent.setup.camIP Property](#)

Use this property to define the IP address of the vRealize Operations Manager server for the agent. The Endpoint Operations Management agent reads this value only in the event that it cannot find connection configuration in its data directory.

- [agent.setup.camLogin Property](#)

At first startup after installation, use this property to define the Endpoint Operations Management agent user name to use when the agent is registering itself with the server.

- [agent.setup.camPort Property](#)

At first startup after installation, use this property to define the Endpoint Operations Management agent server port to use for non-secure communications with the server.

- [agent.setup.camPword Property](#)

Use this property to define the password that the Endpoint Operations Management agent uses when connecting to the vRealize Operations Manager server, so that the agent does not prompt a user to supply the password interactively at first startup.

- [agent.setup.camSecure](#)

This property is used when you are registering the Endpoint Operations Management with the vRealize Operations Manager server to communicate using encryption.

- [agent.setup.camSSLPort Property](#)

At first startup after installation, use this property to define the Endpoint Operations Management agent server port to use for SSL communications with the server.

- [agent.setup.resetupToken Property](#)

Use this property to configure an Endpoint Operations Management agent to create a new token to use for authentication with the server at startup. Regenerating a token is useful if the agent cannot connect to the server because the token has been deleted or corrupted.

- [agent.setup.unidirectional Property](#)

Enables unidirectional communications between the Endpoint Operations Management agent and vRealize Operations Manager server.

- [agent.startupTimeOut Property](#)

The number of seconds that the Endpoint Operations Management agent startup script waits before determining that the agent has not started up successfully. If the agent is found to not be listening for requests within this period, an error is logged, and the startup script times out.

- [autoinventory.defaultScan.interval.millis Property](#)

Specifies how frequently the Endpoint Operations Management agent performs a default autoinventory scan.

- [autoinventory.runtimeScan.interval.millis Property](#)

Specifies how frequently an Endpoint Operations Management agent performs a runtime scan.

- [http.useragent Property](#)

Defines the value for the user-agent request header in HTTP requests issued by the Endpoint Operations Management agent.

- [log4j Properties](#)

The `log4j` properties for the Endpoint Operations Management agent are described here.

- [platform.log\\_track.eventfmt Property](#)

Specifies the content and format of the Windows event attributes that an Endpoint Operations Management agent includes when logging a Windows event as an event in vRealize Operations Manager.

- [plugins.exclude Property](#)

Specifies plug-ins that the Endpoint Operations Management agent does not load at startup. This is useful for reducing an agent's memory footprint.

- [plugins.include Property](#)

Specifies plug-ins that the Endpoint Operations Management agent loads at startup. This is useful for reducing the agent's memory footprint.

- [postgresql.database.name.format Property](#)

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL Database and vPostgreSQL Database database types.

- [postgresql.index.name.format Property](#)

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL Index and vPostgreSQL Index index types.

- [postgresql.server.name.format Property](#)

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL and vPostgreSQL server types.

- [postgresql.table.name.format Property](#)

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL Table and vPostgreSQL Table table types.

- [scheduleThread.cancelTimeout Property](#)

This property specifies the maximum time, in milliseconds, that the ScheduleThread allows a metric collection process to run before attempting to interrupt it.

- [scheduleThread.fetchLogTimeout Property](#)

This property controls when a warning message is issued for a long-running metric collection process.

- [scheduleThread.poolsize Property](#)

This property enables a plug-in to use multiple threads for metric collection. The property can increase metric throughput for plug-ins known to be thread-safe.

- [scheduleThread.queueSize Property](#)

Use this property to limit the metric collection queue size (the number of metrics) for a plug-in.

- [sigar.mirror.procnets Property](#)

mirror /proc/net/tcp on Linux.

- [sigar.pdh.enableTranslation Property](#)

Use this property to enable translation based on the detected locale of the operating system.

- [snmpTrapReceiver.listenAddress Property](#)

Specifies the port on which the Endpoint Operations Management agent listens for SNMP traps

#### agent.keystore.alias Property

This property configures the name of the user-managed keystore for the agent for agents configured for unidirectional communication with the vRealize Operations Manager server.

## Example: Defining the Name of a Keystore

Given this user-managed keystore for a unidirectional agent

```
hq self-signed cert), Jul 27, 2011, trustedCertEntry,
Certificate fingerprint (MD5): 98:FF:B8:3D:25:74:23:68:6A:CB:0B:9C:20:88:74:CE
hq-agent, Jul 27, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5): 03:09:C4:BC:20:9E:9A:32:DC:B2:E8:29:C0:3C:FE:38
```

you define the name of the keystore like this

```
agent.keystore.alias=hq-agent
```

If the value of this property does not match the keystore name, agent-server communication fails.

### Default

The default behavior of the agent is to look for the hq keystore.

For unidirectional agents with user-managed keystores, you must define the keystore name using this property.

### agent.keystore.password Property

This property configures the password for an Endpoint Operations Management agent's SSL keystore.

Define the location of the keystore using the [agent.keystore.path Property](#) property.

By default, the first time you start the Endpoint Operations Management agent following installation, if `agent.keystore.password` is uncommented and has a plain text value, the agent automatically encrypts the property value. You can encrypt this property value yourself, prior to starting the agent.

It is good practice to specify the same password for the agent keystore as for the agent private key.

### Default

By default, the `agent.properties` file does not include this property.

### agent.keystore.path Property

This property configures the location of a Endpoint Operations Management agent's SSL keystore.

Specify the full path to the keystore. Define the password for the keystore using the `agent.keystore.password` property. See [agent.keystore.password Property](#).

### Specifying the Keystore Path on Windows

On Windows platforms, specify the path to the keystore in this format.

```
C:/Documents and Settings/Desktop/keystore
```

### Default

AgentHome/data/keystore.

### agent.listenPort Property

This property specifies the port where the Endpoint Operations Management agent listens to receive communication from the vRealize Operations Manager server.

The property is not required for unidirectional communication.

### agent.logDir Property

You can add this property to the `agent.properties` file to specify the directory where the Endpoint Operations Management agent writes its log file. If you do not specify a fully qualified path, `agent.logDir` is evaluated relative to the agent installation directory.

To change the location for the agent log file, enter a path relative to the agent installation directory, or a fully qualified path.

Note that the name of the agent log file is configured with the `agent.logFile` property.

#### Default

By default, the `agent.properties` file does not include this property.

The default behavior is `agent.logDir=log`, resulting in the agent log file being written to the `AgentHome/Log` directory.

### agent.logFile Property

The path and name of the agent log file.

#### Default

In the `agent.properties` file, the default setting for the `agent.LogFile` property is made up of a variable and a string

```
agent.logFile=${agent.logDir}\agent.log
```

where

- *agent.logDir* is a variable that supplies the value of an identically named agent property. By default, the value of *agent.logDir* is `log`, interpreted relative to the agent installation directory.
- `agent.log` is the name for the agent log file.

By default, the agent log file is named `agent.log`, and is written to the `AgentHome/Log` directory.

### agent.logLevel Property

The level of detail of the messages the agent writes to the log file.

Permitted values are `INFO` and `DEBUG`.

#### Default

`INFO`

### agent.logLevel.SystemErr Property

Redirects `System.err` to the `agent.log` file.

Commenting out this setting causes `System.err` to be directed to `agent.log.startup`.

#### Default

`ERROR`

### agent.logLevel.SystemOut Property

Redirects `System.out` to the `agent.log` file.

Commenting out this setting causes `System.out` to be directed to `agent.log.startup`.

## Default

### INFO

#### agent.proxyHost Property

The host name or IP address of the proxy server that the Endpoint Operations Management agent must connect to first when establishing a connection to the vRealize Operations Manager server.

This property is supported for agents configured for unidirectional communication.

Use this property in conjunction with `agent.proxyPort` and `agent.setup.unidirectional1`.

## Default

### None

#### agent.proxyPort Property

The port number of the proxy server that the Endpoint Operations Management agent must connect to first when establishing a connection to the vRealize Operations Manager server.

This property is supported for agents configured for unidirectional communication.

Use this property in conjunction with `agent.proxyHost` and `agent.setup.unidirectional1`.

## Default

### None

#### agent.setup.acceptUnverifiedCertificate Property

This property controls whether an Endpoint Operations Management agent issues a warning when the vRealize Operations Manager server presents an SSL certificate that is not in the agent's keystore, and is either self-signed or signed by a different certificate authority than the one that signed the agent's SSL certificate.

When the default is used, the agent issues the warning

```
The authenticity of host 'localhost' can't be established.  
Are you sure you want to continue connecting? [default=no]:
```

If you respond **yes**, the agent imports the server's certificate and will continue to trust the certificate from this point on.

## Default

`agent.setup.acceptUnverifiedCertificate=no`

#### agent.setup.camIP Property

Use this property to define the IP address of the vRealize Operations Manager server for the agent. The Endpoint Operations Management agent reads this value only in the event that it cannot find connection configuration in its data directory.

You can specify this and other `agent.setup.*` properties to reduce the user interaction required to configure an agent to communicate with the server.

The value can be provided as an IP address or a fully qualified domain name. To identify an server on the same host as the server, set the value to `127.0.0.1`.

If there is a firewall between the agent and server, specify the address of the firewall, and configure the firewall to forward traffic on port 7080, or 7443 if you use the SSL port, to the vRealize Operations Manager server.

#### Default

Commented out, localhost.

#### agent.setup.camLogin Property

At first startup after installation, use this property to define the Endpoint Operations Management agent user name to use when the agent is registering itself with the server.

The permission required on the server for this initialization is `Create`, for platforms.

Log in from the agent to the server is only required during the initial configuration of the agent.

The agent reads this value only in the event that it cannot find connection configuration in its data directory.

You can specify this and other `agent.setup.*` properties to reduce the user interaction required to configure an agent to communicate with the server.

#### Default

Commented our hqadmin.

#### agent.setup.camPort Property

At first startup after installation, use this property to define the Endpoint Operations Management agent server port to use for non-secure communications with the server.

The agent reads this value only in the event that it cannot find connection configuration in its data directory.

You can specify this and other `agent.setup.*` properties to reduce the user interaction required to configure an agent to communicate with the server.

#### Default

Commented out 7080.

#### agent.setup.camPword Property

Use this property to define the password that the Endpoint Operations Management agent uses when connecting to the vRealize Operations Manager server, so that the agent does not prompt a user to supply the password interactively at first startup.

The password for the user is that specified by `agent.setup.camLogin`.

The agent reads this value only in the event that it cannot find connection configuration in its data directory.

You can specify this and other `agent.setup.*` properties to reduce the user interaction required to configure an agent to communicate with the server.

The first time you start the Endpoint Operations Management agent after installation, if `agent.keystore.password` is uncommented and has a plain text value, the agent automatically encrypts the property value. You can encrypt these property values prior to starting the agent.

## Default

Commented out `hqadmin`.

`agent.setup.camSecure` Property

This property is used when you are registering the Endpoint Operations Management with the vRealize Operations Manager server to communicate using encryption.

Use `yes=secure`, `encrypted`, or `SSL`, as appropriate, to encrypt communication.

Use `no=unencrypted` for unencrypted communication.

`agent.setup.camSSLPort` Property

At first startup after installation, use this property to define the Endpoint Operations Management agent server port to use for SSL communications with the server.

The agent reads this value only in the event that it cannot find connection configuration in its data directory.

You can specify this and other `agent.setup.*` properties to reduce the user interaction required to configure an agent to communicate with the server.

## Default

Commented out 7443.

`agent.setup.resetupToken` Property

Use this property to configure an Endpoint Operations Management agent to create a new token to use for authentication with the server at startup. Regenerating a token is useful if the agent cannot connect to the server because the token has been deleted or corrupted.

The agent reads this value only in the event that it cannot find connection configuration in its data directory.

Regardless of the value of this property, an agent generates a token the first time it is started after installation.

## Default

Commented out `no`.

`agent.setup.unidirectional` Property

Enables unidirectional communications between the Endpoint Operations Management agent and vRealize Operations Manager server.

If you configure an agent for unidirectional communication, all communication with the server is initiated by the agent.

For a unidirectional agent with a user-managed keystore, you must configure the keystore name in the `agent.properties` file.

## Default

Commented out `no`.

`agent.startupTimeOut` Property

The number of seconds that the Endpoint Operations Management agent startup script waits before determining that the agent has not started up successfully. If the agent is found to not be listening for requests within this period, an error is logged, and the startup script times out.

#### Default

By default, the `agent.properties` file does not include this property.

The default behavior of the agent is to timeout after 300 seconds.

#### `autoinventory.defaultScan.interval.millis` Property

Specifies how frequently the Endpoint Operations Management agent performs a default autoinventory scan.

The default scan detects server and platform services objects, typically using the process table or the Windows registry. Default scans are less resource-intensive than runtime scans.

#### Default

The agent performs the default scan at startup and every 15 minutes thereafter.

Commented out 86,400,000 milliseconds, or one day.

#### `autoinventory.runtimeScan.interval.millis` Property

Specifies how frequently an Endpoint Operations Management agent performs a runtime scan.

A runtime scan may use more resource-intensive methods to detect services than a default scan. For example, a runtime scan might involve issuing an SQL query or looking up an MBean.

#### Default

86,400,000 milliseconds, or one day.

#### `http.useragent` Property

Defines the value for the user-agent request header in HTTP requests issued by the Endpoint Operations Management agent.

You can use `http.useragent` to define a user-agent value that is consistent across upgrades.

By default, the `agent.properties` file does not include this property.

#### Default

By default, the user-agent in agent requests includes the Endpoint Operations Management agent version, so changes when the agent is upgraded. If a target HTTP server is configured to block requests with an unknown user-agent, agent requests fail after an agent upgrade.

Hyperic-HQ-Agent/Version, for example, Hyperic-HQ-Agent/4.1.2-EE.

#### log4j Properties

The log4j properties for the Endpoint Operations Management agent are described here.

```
log4j.rootLogger=${agent.logLevel}, R

log4j.appender.R.File=${agent.logFile}
log4j.appender.R.MaxBackupIndex=1
log4j.appender.R.MaxFileSize=5000KB
log4j.appender.R.layout.ConversionPattern=%d{dd-MM-yyyy HH:mm:ss,SSS z} %-5p [%t] [%c{1}@%L] %m%n
```

```

log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R=org.apache.log4j.RollingFileAppender

##
## Disable overly verbose logging
##
log4j.logger.org.apache.http=ERROR
log4j.logger.org.springframework.web.client.RestTemplate=ERROR
log4j.logger.org.hyperic.hq.measurement.agent.server.SenderThread=INFO
log4j.logger.org.hyperic.hq.agent.server.AgentDLListProvider=INFO
log4j.logger.org.hyperic.hq.agent.server.MeasurementSchedule=INFO
log4j.logger.org.hyperic.util.units=INFO
log4j.logger.org.hyperic.hq.product.pluginxml=INFO

# Only log errors from naming context
log4j.category.org.jnp.interfaces.NamingContext=ERROR
log4j.category.org.apache.axis=ERROR

#Agent Subsystems: Uncomment individual subsystems to see debug messages.
#-----
#log4j.logger.org.hyperic.hq.autoinventory=DEBUG
#log4j.logger.org.hyperic.hq.livedata=DEBUG
#log4j.logger.org.hyperic.hq.measurement=DEBUG
#log4j.logger.org.hyperic.hq.control=DEBUG

#Agent Plugin Implementations
#log4j.logger.org.hyperic.hq.product=DEBUG

#Server Communication
#log4j.logger.org.hyperic.hq.bizapp.client.AgentCallbackClient=DEBUG

#Server Realtime commands dispatcher
#log4j.logger.org.hyperic.hq.agent.server.CommandDispatcher=DEBUG

#Agent Configuration parser
#log4j.logger.org.hyperic.hq.agent.AgentConfig=DEBUG

#Agent plugins loader
#log4j.logger.org.hyperic.util.PluginLoader=DEBUG

#Agent Metrics Scheduler (Scheduling tasks definitions & executions)
#log4j.logger.org.hyperic.hq.agent.server.session.AgentSynchronizer.SchedulerThread=DEBUG

#Agent Plugin Managers
#log4j.logger.org.hyperic.hq.product.MeasurementPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.AutoinventoryPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.ConfigTrackPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.LogTrackPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.LiveDataPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.ControlPluginManager=DEBUG

```

platform.log\_track.eventfmt Property

Specifies the content and format of the Windows event attributes that an Endpoint Operations Management agent includes when logging a Windows event as an event in vRealize Operations Manager.

By default, the `agent.properties` file does not include this property.

#### Default

When Windows log tracking is enabled, an entry in the form `[Timestamp] Log Message (EventLogName):EventLogName:EventAttributes` is logged for events that match the criteria you specified on the resource's Configuration Properties page.

Attribute	Description
Timestamp	When the event occurred
Log Message	A text string
EventLogName	The Windows event log type System, Security, or Application
EventAttributes	A colon delimited string made of the Windows event Source and Message attributes

For example, the log entry: `04/19/2010 06:06 AM Log Message (SYSTEM): SYSTEM: Print: Printer HP LaserJet 6P was paused.` is for a Windows event written to the Windows System event log at 6:06 AM on 04/19/2010. The Windows event Source and Message attributes, are "Print" and "Printer HP LaserJet 6P was paused.", respectively.

#### Configuration

Use the following parameters to configure the Windows event attributes that the agent writes for a Windows event. Each parameter maps to Windows event attribute of the same name.

Parameter	Description
<code>%user%</code>	The name of the user on whose behalf the event occurred.
<code>%computer%</code>	The name of the computer on which the event occurred.
<code>%source%</code>	The software that logged the Windows event.
<code>%event%</code>	A number identifying the particular event type.
<code>%message%</code>	The event message.
<code>%category%</code>	An application-specific value used for grouping events.

For example, with the property setting `platform.log_track.eventfmt=%user%%computer% %source %:%event%:%message%`, the Endpoint Operations Management agent writes the following data when logging the Windows event `04/19/2010 06:06 AM Log Message (SYSTEM): SYSTEM: HP_Administrator@Office Print:7:Printer HP LaserJet 6P was paused..` This entry is for a Windows event written to the Windows system event log at 6:06 AM on 04/19/2010. The software associated with the event was running as "HP\_Administrator" on the host "Office". The Windows event's Source, Event, and Message attributes, are "Print", "7", and "Printer HP LaserJet 6P was paused.", respectively.

#### plugins.exclude Property

Specifies plug-ins that the Endpoint Operations Management agent does not load at startup. This is useful for reducing an agent's memory footprint.

## Usage

Supply a comma-separated list of plug-ins to exclude. For example,

```
plugins.exclude=jboss,apache,mysql
```

### plugins.include Property

Specifies plug-ins that the Endpoint Operations Management agent loads at startup. This is useful for reducing the agent's memory footprint.

## Usage

Supply a comma-separated list of plug-ins to include. For example,

```
plugins.include=weblogic,apache
```

### postgresql.database.name.format Property

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL Database and vPostgreSQL Database database types.

By default, the name of a PostgreSQL or vPostgreSQL database is Database *DatabaseName*, where *DatabaseName* is the auto-discovered name of the database.

To use a different naming convention, define `postgresql.database.name.format`. The variable data you use must be available from the PostgreSQL plug-in.

Use the following syntax to specify the default table name assigned by the plug-in,

```
Database ${db}
```

where

`postgresql.db` is the auto-discovered name of the PostgreSQL or vPostgreSQL database.

## Default

By default, the `agent.properties` file does not include this property.

### postgresql.index.name.format Property

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL Index and vPostgreSQL Index index types.

By default, the name of a PostgreSQL or vPostgreSQL index is Index *DatabaseName.Schema.Index*, comprising the following variables

Variable	Description
DatabaseName	The auto-discovered name of the database.
Schema	The auto-discovered schema for the database.
Index	The auto-discovered name of the index.

To use a different naming convention, define `postgresql.index.name.format`. The variable data you use must be available from the PostgreSQL plug-in.

Use the following syntax to specify the default index name assigned by the plug-in,

```
Index ${db}.${schema}.${index}
```

where

Attribute	Description
db	Identifies the platform that hosts the PostgreSQL or vPostgreSQL server.
schema	Identifies the schema associated with the table.
index	The index name in PostgreSQL.

### Default

By default, the `agent.properties` file does not include this property.

#### postgresql.server.name.format Property

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL and vPostgreSQL server types.

By default, the name of a PostgreSQL or vPostgreSQL server is *Host:Port*, comprising the following variables

Variable	Description
Host	The FQDN of the platform that hosts the server.
Port	The PostgreSQL listen port.

To use a different naming convention, define `postgresql.server.name.format`. The variable data you use must be available from the PostgreSQL plug-in.

Use the following syntax to specify the default server name assigned by the plug-in,

```
${postgresql.host}:${postgresql.port}
```

where

Attribute	Description
postgresql.host	Identifies the FQDN of the hosting platform.
postgresql.port	Identifies the database listen port.

### Default

By default, the `agent.properties` file does not include this property.

#### postgresql.table.name.format Property

This property specifies the format of the name that the PostgreSQL plug-in assigns to auto-discovered PostgreSQL Table and vPostgreSQL Table table types.

By default, the name of a PostgreSQL or vPostgreSQL table is Table *DatabaseName.Schema.Table*, comprising the following variables

Variable	Description
DatabaseName	The auto-discovered name of the database.
Schema	The auto-discovered schema for the database.
Table	The auto-discovered name of the table.

To use a different naming convention, define `postgresql.table.name.format`. The variable data you use must be available from the PostgreSQL plug-in.

Use the following syntax to specify the default table name assigned by the plug-in,

```
Table ${db}.${schema}.${table}
```

where

Attribute	Description
db	Identifies the platform that hosts the PostgreSQL or vPostgreSQL server.
schema	Identifies the schema associated with the table.
table	The table name in PostgreSQL.

## Default

By default, the `agent.properties` file does not include this property.

### `scheduleThread.cancelTimeout` Property

This property specifies the maximum time, in milliseconds, that the `ScheduleThread` allows a metric collection process to run before attempting to interrupt it.

When the timeout is exceeded, collection of the metric is interrupted, if it is in a `wait()`, `sleep()` or non-blocking `read()` state.

### Usage

```
scheduleThread.cancelTimeout=5000
```

### Default

5000 milliseconds.

### `scheduleThread.fetchLogTimeout` Property

This property controls when a warning message is issued for a long-running metric collection process.

If a metric collection process exceeds the value of this property, which is measured in milliseconds, the agent writes a warning message to the `agent.log` file.

### Usage

```
scheduleThread.fetchLogTimeout=2000
```

### Default

2000 milliseconds.

### `scheduleThread.poolsize` Property

This property enables a plug-in to use multiple threads for metric collection. The property can increase metric throughput for plug-ins known to be thread-safe.

## Usage

Specify the plug-in by name and the number of threads to allocate for metric collection

```
scheduleThread.poolsize.PluginName=2
```

where *PluginName* is the name of the plug-in to which you are allocating threads. For example,

```
scheduleThread.poolsize.vsphere=2
```

## Default

1

scheduleThread.queueSize Property

Use this property to limit the metric collection queue size (the number of metrics) for a plug-in.

## Usage

Specify the plug-in by name and the maximum metric queue length number:

```
scheduleThread.queueSize.PluginName=15000
```

where *PluginName* is the name of the plug-in on which you are imposing a metric limit.

For example,

```
scheduleThread.queueSize.vsphere=15000
```

## Default

1000

sigar.mirror.procnets Property

mirror /proc/net/tcp on Linux.

## Default

true

sigar.pdh.enableTranslation Property

Use this property to enable translation based on the detected locale of the operating system.

snmpTrapReceiver.listenAddress Property

Specifies the port on which the Endpoint Operations Management agent listens for SNMP traps

By default, the `agent.properties` file does not include this property.

Typically SNMP uses the UDP port 162 for trap messages. This port is in the privileged range, so an agent listening for trap messages on it must run as `root`, or as an administrative user on Windows.

You can run the agent in the context of a non-administrative user, by configuring the agent to listen for trap messages on an unprivileged port.

## Usage

Specify an IP address (or 0.0.0.0 to specify all interfaces on the platform) and the port for UDP communications in the format

```
snmpTrapReceiver.listenAddress=udp:IP_address/port
```

To enable the Endpoint Operations Management agent to receive SNMP traps on an unprivileged port, specify port 1024 or higher. The following setting allows the agent to receive traps on any interface on the platform, on UDP port 1620.

```
snmpTrapReceiver.listenAddress=udp:0.0.0.0/1620
```

## Managing Agent Registration on vRealize Operations Manager Servers

The Endpoint Operations Management agents identify themselves to the server using client certificates. The agent registration process generates the client certificate.

The client certificate includes a token that is used as the unique identifier. If you suspect that a client certificate was stolen or compromised, you must replace the certificate.

You must have AgentManager credentials to perform the agent registration process.

If you remove and reinstall an agent by removing the data directory, the agent token is retained to enable data continuity. See [Understanding Agent Uninstallation and Reinstallation Implications](#).

### Regenerate an Agent Client Certificate

An Endpoint Operations Management agent client certificate might expire and need to be replaced. For example, you would replace a certificate that you suspected was corrupt or compromised.

#### Prerequisites

Verify that you have sufficient privileges to deploy an Endpoint Operations Management agent. You must have vRealize Operations Manager user credentials that include a role that allows you to install Endpoint Operations Management agents. See [Roles and Privileges in vRealize Operations Manager](#).

#### Procedure

- ◆ Start the registration process by running the setup command that is appropriate for the operating system on which the agent is running.

Operating System	Run Command
Linux	ep-agent.sh setup
Windows	ep-agent.bat setup

The agent installer runs the setup, requests a new certificate from the server, and imports the new certificate to the keystore.

## Securing Communications with the Server

Communication from an Endpoint Operations Management agent to the vRealize Operations Manager server is unidirectional, however both parties must be authenticated. Communication is always secured using transport layer security (TLS).

The first time an agent initiates a connection to the vRealize Operations Manager server following installation, the server presents its SSL certificate to the agent.

If the agent trusts the certificate that the server presented, the agent imports the server's certificate to its own keystore.

The agent trusts a server certificate if that certificate, or one of its issuers (CA) already exists in the agent's keystore.

By default, if the agent does not trust the certificate that the server presents, the agent issues a warning. You can choose to trust the certificate, or to terminate the configuration process. The vRealize Operations Manager server and the agent do not import untrusted certificates unless you respond yes to the warning prompt.

You can configure the agent to accept a specific thumb print without warning by specifying the thumb print of the certificate for the vRealize Operations Manager server.

By default, the vRealize Operations Manager server generates a self-signed CA certificate that is used to sign the certificate of all the nodes in the cluster. In this case, the thumbprint must be the thumbprint of the issuer, to allow for the agent to communicate with all nodes.

As a vRealize Operations Manager administrator, you can import a custom certificate instead of using the default. In this instance, you must specify a thumbprint corresponding to that certificate as the value of this property.

Either the SHA1 or SHA256 algorithm can be used for the thumbprint.

## Launching Agents from a Command Line

You can launch agents from a command line on both Linux and Windows operating systems.

Use the appropriate process for your operating system.

If you are deleting the data directory, do not use Windows Services to stop and start an Endpoint Operations Management agent. Stop the agent using `epops-agent.bat stop`. Delete the data directory, then start the agent using `epops-agent.bat start`.

### Run the Agent Launcher from a Linux Command Line

You can initiate the agent launcher and agent lifecycle commands with the `epops-agent.sh` script in the `AgentHome/bin` directory.

#### Procedure

- 1 Open a command shell or terminal window.

- 2 Enter the required command, using the format `sh epops-agent.sh command`, where *command* is one of the following.

Option	Description
<b>start</b>	Starts the agent as a daemon process.
<b>stop</b>	Stops the agent's JVM process.
<b>restart</b>	Stops and then starts the agent's JVM process.
<b>status</b>	Queries the status of the agent's JVM process.
<b>dump</b>	Runs a thread dump for the agent process, and writes the result to the <code>agent.log</code> file in <code>AgentHome/Log</code> .
<b>ping</b>	Pings the agent process.
<b>setup</b>	Re-registers the certificate using the existing token.

### Run the Agent Launcher from a Windows Command Line

You can initiate the agent launcher and agent lifecycle commands with the `epops-agent.bat` script in the `AgentHome/bin` directory.

#### Procedure

- 1 Open a terminal window.
- 2 Enter the required command, using the format `epops-agent.bat command`, where *command* is one of the following.

Option	Description
<b>install</b>	Installs the agent NT service. You must run <code>start</code> after running <code>install</code> .
<b>start</b>	Starts the agent as an NT service.
<b>stop</b>	Stops the agent as an NT service.
<b>remove</b>	Removes the agent's service from the NT service table.
<b>query</b>	Queries the current status of the agent NT service ( <code>status</code> ).
<b>dump</b>	Runs a thread dump for the agent process, and writes the result to the <code>agent.log</code> file in <code>AgentHome/Log</code> .
<b>ping</b>	Pings the agent process.
<b>setup</b>	Re-registers the certificate using the existing token.

### Managing an Endpoint Operations Management Agent on a Cloned Virtual Machine

When you clone a virtual machine that is running an Endpoint Operations Management agent that is collecting data, there are processes that you must complete related to data continuity to ensure data continuity.

## Cloning a Virtual Machine to Delete the Original Virtual Machine

If you are cloning the virtual machine so that you can delete the original virtual machine, you need to verify that the original machine is deleted from the vCenter Server and from vRealize Operations Manager so that the new operating system to virtual machine relationship can be created.

## Cloning a Virtual Machine to Run Independently of the Original Machine

If you are cloning the virtual machine so that you can run the two machines independently of the other, the cloned machine requires a new agent because an agent can only monitor a single machine.

### Procedure

- ◆ On the cloned machine, delete the Endpoint Operations Management token and the data folder, according to the operating system of the machine.

Operating System	Process
Linux	Delete the Endpoint Operations Management token and the data folder.
Windows	<ol style="list-style-type: none"> <li>1 Run <code>epops-agent remove</code>.</li> <li>2 Remove the agent token and the data folder.</li> <li>3 Run <code>epops-agent install</code>.</li> <li>4 Run <code>epops-agent start</code>.</li> </ol>

## Moving Virtual Machines between vCenter Server Instances

When you move a virtual machine from one vCenter Server to another, you must delete the original machine from vRealize Operations Manager to enable the new operating system relationship with the virtual machine to be created.

## Understanding Agent Uninstallation and Reinstallation Implications

When you uninstall or reinstall an Endpoint Operations Management agent, various elements are affected, including existing metrics that the agent has collected, and the identification token that enables a reinstalled agent to report on the previously discovered objects on the server. To ensure that you maintain data continuity, it is important that you are aware of the implications of uninstalling and reinstalling an agent.

There are two key locations related to the agent that are preserved when you uninstall an agent. Before reinstalling the agent, you must decide whether to retain or delete the files.

- The `/data` folder is created during agent installation. It contains the keystore, unless you chose a different location for it, and other data related to the currently installed agent.
- The `epops-token` platform token file is created before agent registration and is stored as follows:
  - Linux: `/etc/vmware/epops-token`
  - Windows: `%PROGRAMDATA%/VMware/EP Ops Agent/epops-token`

When you uninstall an agent, you must delete the `/data` folder. This does not affect data continuity.

However, to enable data continuity it is important that you do not delete the `epops-token` file. This file contains the identity token for the platform object. Following agent reinstallation, the token enables the agent to be synchronized with the previously discovered objects on the server.

When you reinstall the agent, the system notifies you whether it found an existing token, and provides its identifier. If a token is found, the system uses that token. If a token is not found, the system creates a new one. In the case of an error, the system prompts you to provide either a location and file name for the existing token file, or a location and file name for a new one.

The method that you use to uninstall an agent depends on how it was installed.

- **Uninstall an Agent that was Installed from an Archive**

You can use this procedure to uninstall agents that you installed on virtual machines in your environment from an archive.

- **Uninstall an Agent that was Installed Using an RPM Package**

You can use this procedure to uninstall agents that you installed on virtual machines in your environment using an RPM package.

- **Uninstall an Agent that was Installed Using a Windows Executable**

You can use this procedure to uninstall agents that you installed on virtual machines in your environment from a Windows EXE file.

- **Reinstall an Agent**

If you change the IP address, hostname or port number of the vRealize Operations Manager server, you need to uninstall and reinstall your agents.

### **Uninstall an Agent that was Installed from an Archive**

You can use this procedure to uninstall agents that you installed on virtual machines in your environment from an archive.

#### **Prerequisites**

Verify that the agent is stopped.

#### **Procedure**

- 1 (Optional) If you have a Windows operating system, run `ep-agent.bat remove` to remove the agent service.
- 2 Select the uninstall option that is appropriate to your situation.
  - If you do not intend to reinstall the agent after you have uninstalled it, delete the agent directory. The default name of the directory is `epops-agent-version`.
  - If you are reinstalling the agent after you have uninstalled it, delete the `/data` directory.

- 3 (Optional) If you do not intend to reinstall the agent after you have uninstalled it, or you do not need to maintain data continuity, delete the `epops-token` platform token file.

Depending on your operating system, the file to delete is one of the following, unless otherwise defined in the properties file.

- Linux: `/etc/epops/epops-token`
- Windows: `%PROGRAMDATA%/VMware/EP Ops Agent/epops-token`

### Uninstall an Agent that was Installed Using an RPM Package

You can use this procedure to uninstall agents that you installed on virtual machines in your environment using an RPM package.

When you are uninstalling an Endpoint Operations Management agent, it is good practice to stop the agent running, to reduce unnecessary load on the server.

#### Procedure

- ◆ On the virtual machine from which you are removing the agent, open a command line and run `rpm -e epops-agent`.

The agent is uninstalled from the virtual machine.

### Uninstall an Agent that was Installed Using a Windows Executable

You can use this procedure to uninstall agents that you installed on virtual machines in your environment from a Windows EXE file.

When you are uninstalling an Endpoint Operations Management agent, it is good practice to stop the agent running, to reduce unnecessary load on the server.

#### Procedure

- ◆ Double-click `unins000.exe` in the installation destination directory for the agent.

The agent is uninstalled from the virtual machine.

### Reinstall an Agent

If you change the IP address, hostname or port number of the vRealize Operations Manager server, you need to uninstall and reinstall your agents.

#### Prerequisites

To maintain data continuity, you must have retained the `epops-token` platform token file when you uninstalled your agent. See [Uninstall an Agent that was Installed from an Archive](#).

When you reinstall an Endpoint Operations Management agent on a virtual machine, objects that had previously been detected are no longer monitored. To avoid this situation, do not restart the Endpoint Operations Management agent until the plug-in synchronization is complete.

**Procedure**

- ◆ Run the agent install procedure that is relevant to your operating system.

See [Selecting an Agent Installer Package](#).

**What to do next**

After you reinstall an agent, MSSQL resources might stop receiving data. If this happens, edit the problematic resources and click **OK**.

**Install Multiple Endpoint Operations Management Agents Simultaneously**

If you have multiple Endpoint Operations Management agents to install at one time, you can create a single standardized `agent.properties` file that all the agents can use.

Installing multiple agents entails a number of steps. Perform the steps in the order listed.

**Prerequisites**

Verify that the following prerequisites are satisfied.

- 1 Set up an installation server.

An installation server is a server that can access the target platforms from which to perform remote installation.

The server must be configured with a user account that has permissions to SSH to each target platform without requiring a password.

- 2 Verify that each target platform on which an Endpoint Operations Management agent will be installed has the following items.
  - A user account that is identical to that created on the installation server.
  - An identically named installation directory, for example `/home/epomagent`.
  - A trusted keystore, if required.

**Procedure**

- 1 [Create a Standard Endpoint Operations Management Agent Properties File](#)

You can create a single properties file that contains property values that multiple agents use .

- 2 [Deploy and Start Multiple Agents One-By-One](#)

You can perform remote installations to deploy multiple agents that use a single `agent.properties` file one-by-one.

- 3 [Deploy and Start Multiple Agents Simultaneously](#)

You can perform remote installations to simultaneously deploy agents that use a single `agent.properties` file.

**Create a Standard Endpoint Operations Management Agent Properties File**

You can create a single properties file that contains property values that multiple agents use .

To enable multiple agent deployment, you create an `agent.properties` file that defines the agent properties required for the agent to start up and connect with the vRealize Operations Manager server. If you supply the necessary information in the properties file, each agent locates its setup configuration at startup, rather than prompting you for the location. You can copy the agent properties file to the agent installation directory, or to a location available to the installed agent.

### Prerequisites

Verify that the prerequisites in [Install Multiple Endpoint Operations Management Agents Simultaneously](#) are satisfied.

### Procedure

- 1 Create an `agent.properties` file in a directory.

You will copy this file later to other machines.

- 2 Configure the properties as required.

The minimum configuration is the IP address, user name, password, thumb print, and port of the vRealize Operations Manager installation server.

- 3 Save your configurations.

The first time that the agents are started, they read the `agent.properties` file to identify the server connection information. The agents connect to the server and register themselves.

### What to do next

Perform remote agent installations. See [Deploy and Start Multiple Agents One-By-One](#) or [Deploy and Start Multiple Agents Simultaneously](#).

### Deploy and Start Multiple Agents One-By-One

You can perform remote installations to deploy multiple agents that use a single `agent.properties` file one-by-one.

### Prerequisites

- Verify that the prerequisites in [Install Multiple Endpoint Operations Management Agents Simultaneously](#) are satisfied.
- Verify that you configured a standard agent properties file and copied it to the agent installation, or to a location available to the agent installation.

### Procedure

- 1 Log in to the installation server user account that you configured with permissions to use SSH to connect to each target platform without requiring a password.
- 2 Use SSH to connect to the remote platform.
- 3 Copy the agent archive to the agent host.
- 4 Unpack the agent archive.

- 5 Copy the `agent.properties` file to the `AgentHome/conf` directory of the unpacked agent archive on the remote platform.
- 6 Start the new agent.

The agent registers with the vRealize Operations Manager server and the agent runs an autodiscovery scan to discover its host platform and supported managed products that are running on the platform.

### Deploy and Start Multiple Agents Simultaneously

You can perform remote installations to simultaneously deploy agents that use a single `agent.properties` file.

#### Prerequisites

- Verify that the prerequisites in [Install Multiple Endpoint Operations Management Agents Simultaneously](#) are satisfied.
- Verify that you configured a standard agent properties file and copied it to the agent installation, or to a location available to the agent installation. See [Create a Standard Endpoint Operations Management Agent Properties File](#).

#### Procedure

- 1 Create a `hosts.txt` file on your installation server that maps the hostname to the IP address of each platform on which you are installing an agent.
- 2 Open a command-line shell on the installation server.
- 3 Type the following command in the shell, supplying the correct name for the agent package in the `export` command.

```
$ export AGENT=epops-agent-x86-64-linux-1.0.0.tar.gz
$ export PATH_TO_AGENT_INSTALL=</path/to/agent/install>
$ for host in `cat hosts.txt`; do scp $AGENT $host:$PATH_TO_AGENT_INSTALL && ssh $host "cd
$PATH_TO_AGENT_INSTALL; tar xzfp $AGENT &&
./epops-agent-1.0.0/ep-agent.sh start"; done
```

- 4 (Optional) If the target hosts have sequential names, for example `host001`, `host002`, `host003`, and so on, you can skip the `hosts.txt` file and use the `seq` command.

```
$ export AGENT=epops-agent-x86-64-linux-1.0.0.tar.gz
$ for i in `seq 1 9`; do scp $AGENT host$i: && ssh host$i "tar xzfp $AGENT &&
./epops-agent-1.0.0/ep-agent.sh start"; done
```

The agents register with the vRealize Operations Manager server and the agents run an autodiscovery scan to discover their host platform and supported managed products that are running on the platform.

### Upgrade the Endpoint Operations Management Agent

You can upgrade the 6.3 or 6.4 version of an Endpoint Operations Management agent to a 6.5 version from the vRealize Operations Manager administration interface.

## Prerequisites

- Download the Endpoint Operations Management PAK file.
- Before you install the PAK file, or upgrade your vRealize Operations Manager instance, clone any customized content to preserve it. Customized content can include alert definitions, symptom definitions, recommendations, and views. Then, during the software update, you select the options named **Install the PAK file even if it is already installed** and **Reset out-of-the-box content**.

## Procedure

- 1 Log into the vRealize Operations Manager administration interface of your cluster at `https://IP-address/admin`.
- 2 Click **Software Update** in the left panel.
- 3 Click **Install a Software Update** in the main panel.
- 4 From the **Add Software Update** dialog box, click **Browse** to select the PAK file.
- 5 Click **Upload** and follow the steps in the wizard to install your PAK file.
- 6 After Step 4 of the install is complete, you return to the Software Update page of the Endpoint Operations Management administration interface.
- 7 A message that indicates that the software update completed successfully appears in the main pane.  
If any of the agents have not installed successfully, rerun the upgrade steps and ensure that you have selected **Install the PAK file even if it is already installed** in the Add Software Update - Select Software Update page.

## What to do next

You can view the log files from the vRealize Operations Manager administration interface > Support page.

## Access and View the Log Files

You can access and view the log files to troubleshoot agent upgrade failure. You can verify the status of the agents during and after the upgrade process to find out if the agents have upgraded successfully.

You can view the status of the agents during the upgrade from the `epops-agent-upgrade-status.txt` file. You can view a final report of the number of agents that have successfully upgraded or failed upgrade from the `epops-agent-bundle-upgrade-summary.txt` file.

## Procedure

- 1 Log into the vRealize Operations Manager administration interface of your cluster at `https://IP-address/admin`.
- 2 Click **Support** in the left panel.
- 3 Click the **Logs** tab in the right pane and double-click **EPOPS**.
- 4 Double-click the log file to view the contents.

## Roles and Privileges in vRealize Operations Manager

vRealize Operations Manager provides several predefined roles to assign privileges to users. You can also create your own roles.

You must have privileges to access specific features in the vRealize Operations Manager user interface. The roles associated with your user account determine the features you can access and the actions you can perform.

Each predefined role includes a set of privileges for users to perform create, read, update, or delete actions on components such as dashboards, reports, administration, capacity, policies, problems, symptoms, alerts, user account management, and adapters.

<b>Administrator</b>	Includes privileges to all features, objects, and actions in vRealize Operations Manager.
<b>PowerUser</b>	Users have privileges to perform the actions of the Administrator role except for privileges to user management and cluster management. vRealize Operations Manager maps vCenter Server users to this role.
<b>PowerUserMinusRemediation</b>	Users have privileges to perform the actions of the Administrator role except for privileges to user management, cluster management, and remediation actions.
<b>ContentAdmin</b>	Users can manage all content, including views, reports, dashboards, and custom groups in vRealize Operations Manager.
<b>AgentManager</b>	Users can deploy and configure Endpoint Operations Management agents.
<b>GeneralUser-1 through GeneralUser-4</b>	These predefined template roles are initially defined as ReadOnly roles. vCenter Server administrators can configure these roles to create combinations of roles to give users multiple types of privileges. Roles are synchronized to vCenter Server once during registration.
<b>ReadOnly</b>	Users have read-only access and can perform read operations, but cannot perform write actions such as create, update, or delete.

## Registering Agents on Clusters

You can streamline the process of registering agents on clusters by defining a DNS name for a cluster and configuring that cluster so that the metrics are shared sequentially in a loop.

You only need to register the agent on the DNS, not on the IP address of each individual machine in the cluster. If you do register the agent on each node in the cluster, it affects the scale of your environment.

When you have configured the cluster so that the received metrics are shared in a sequential loop, each time that the agent queries the DNS server for an IP address, the returned address is for one of the virtual machines in the cluster. The next time the agent queries the DNS, it sequentially supplies the IP address of the next virtual machine in the cluster, and so on. The clustered machines are set up in a loop configuration so that each machine receives metrics in turn, ensuring a balanced load.

After you configure the DNS, it is important to maintain it, ensuring that when machines are added or removed from the cluster, their IP address information is updated accordingly.

## Manually Create Operating System Objects

The agent automatically discovers some of the objects to monitor. You can manually add other objects, such as files, scripts or processes, and specify the details so that the agent can monitor them.

The **Monitor OS Object** action only appears in the **Actions** menu of a object that can be a parent object.

### Procedure

1 In the left pane of vRealize Operations Manager, select the agent adapter object that is to be the parent under which you are creating an OS object.

2 Select **Actions > Monitor OS Object**.

A list of parent object context-sensitive objects appear in the menu.

3 Choose one of the following options.

- Click an object type from the list to open the Monitor OS Object dialog for that object type.

The three most popularly selected object types appear in the list.

- If the object type that you want to select is not in the list, click **More** to open the Monitor OS Object dialog, and select the object type from the complete list of objects that are available for selection in the **Object Type** menu.

4 Specify a display name for the OS object.

5 Enter the appropriate values in the other text boxes.

The options in the menu are filtered according to the OS object type that you select.

Some text boxes might display default values, which you can overwrite if necessary. Note the following information about default values.

Option	Value
Process	<p>Supply the PTQL query in the form: <code>Class.Attribute.operator=value</code>.            For example, <code>Pid.PidFile.eq=/var/run/sshd.pid</code>.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>■ <code>Class</code> is the name of the Sigar class without the Proc prefix.</li> <li>■ <code>Attribute</code> is an attribute of the given Class, index into an array or key in a Map class.</li> <li>■ <code>operator</code> is one of the following (for String values):               <ul style="list-style-type: none"> <li>■ <code>eq</code> Equal to value</li> <li>■ <code>ne</code> Not Equal to value</li> <li>■ <code>ew</code> Ends with value</li> <li>■ <code>sw</code> Starts with value</li> <li>■ <code>ct</code> Contains value (substring)</li> <li>■ <code>re</code> Regular expression value matches</li> </ul> </li> </ul> <p>Delimit queries with a comma.</p>
Windows Service	<p>Monitor an application that runs as a service under Windows.</p> <p>To configure it, you supply its Service Name in Windows.</p> <p>To determine the Service Name:</p> <ol style="list-style-type: none"> <li>1 Select <b>Run</b> from the Windows Start menu.</li> <li>2 Type <code>services.msc</code> in the run dialog and click <b>OK</b>.</li> <li>3 In the list of services displayed, right-click the service to monitor and choose <b>Properties</b>.</li> <li>4 Locate the Service Name on the <b>General</b> tab.</li> </ol>
Script	Configure vRealize Operations Manager to periodically run a script that collects a system or application metric.

## 6 Click **OK**.

You cannot click **OK** until you enter values for all the mandatory text boxes.

The OS object appears under its parent object and monitoring begins.

**Caution** If you enter invalid details when you create an OS object, the object is created but the agent cannot discover it, and metrics are not collected.

## Managing Objects with Missing Configuration Parameters

Sometimes when an object is discovered by vRealize Operations Manager for the first time, the absence of values for some mandatory configuration parameters is detected. You can edit the object's parameters to supply the missing values.

If you select **Custom Groups > Objects with Missing Configuration (EP Ops)** in the Environment Overview view of vRealize Operations Manager, you can see the list of all objects that have missing mandatory configuration parameters. In addition, objects with such missing parameters return an error in the Collection Status data.

If you select an object in the vRealize Operations Manager user interface that has missing configuration parameters, the red Missing Configuration State icon appears on the menu bar. When you point to the icon, details about the specific issue appear.

You can add the missing parameter values through the **Action > Edit Object** menu.

## Mapping Virtual Machines to Operating Systems

You can map your virtual machines to an operating system to provide additional information to assist you to determine the root cause of why an alert was triggered for a virtual machine.

vRealize Operations Manager monitors your ESXi hosts and the virtual machines located on them. When you deploy an Endpoint Operations Management agent, it discovers the virtual machines and the objects that are running on them. By correlating the virtual machines discovered by the Endpoint Operations Management agent with the operating systems monitored by vRealize Operations Manager you have more details to determine the exact cause of an alert being triggered.

Verify that you have the vCenter Adapter configured with the vCenter Server that manages the virtual machines. You also need to ensure that you have VMware Tools that are compatible with the vCenter Server installed on each of the virtual machines.

### User Scenario

vRealize Operations Manager is running but you have not yet deployed the Endpoint Operations Management agent in your environment. You configured vRealize Operations Manager to send you alerts when CPU problems occur. You see an alert on your dashboard because insufficient CPU capacity is available on one of your virtual machines that is running a Linux operating system. You deploy another two virtual CPUs but the alert remains. You struggle to determine what is causing the problem.

In the same situation, if you deployed the Endpoint Operations Management agent, you can see the objects on your virtual machines, and determine that an application-type object is using all available CPU capacity. When you add more CPU capacity, it also uses that. You disable the object and your CPU availability is no longer a problem.

### Viewing Objects on Virtual Machines

After you deploy an Endpoint Operations Management agent on a virtual machine, the machine is mapped to the operating system and you can see the objects on that machine.

All the actions and the views that are available to other objects in your vRealize Operations Manager environment are also available for newly discovered server, service, and application objects, and for the deployed agent.

You can see the objects on a virtual machine in the inventory when you select the machine in the **Environment > vSphere Hosts and Clusters** view. You can see the objects and the deployed agent under the operating system.

When you select an object, the center pane of the user interface displays data relevant to that objects.

## Customizing How Endpoint Operations Management Monitors Operating Systems

Endpoint Operations Management gathers operating system metrics through agent-based collections. In addition to the features available after initial configuration of Endpoint Operations Management, you can enable remote monitoring, enable or disable plug-ins for additional monitoring, and customize Endpoint Operations Management logging.

## Configuring Remote Monitoring

With remote monitoring you can monitor the state of an object from a remote location by configuring a remote check.

You can configure remote monitoring using HTTP, ICMP TCP methods.

When you configure a remote HTTP, ICMP or TCP check, it is created as a child object of the tested object that you are monitoring and of the monitoring agent.

If the object that you select to remotely monitor does not already have an alert configured, one is created automatically in the format *Remote check type failed on a object type*. If the object has an existing alert, that is used.

### Configure Remote Monitoring of an Object

Use this procedure to configure remote monitoring of an object.

Configuration options are defined in [HTTP Configuration Options](#), [ICMP Configuration Options](#) and [TCP Configuration Options](#). You might need to refer to this information when you are completing this procedure.

#### Procedure

- 1 In the vRealize Operations Manager user interface, select the remote object to monitor.
- 2 On the details page for the object, select **Monitor this Object Remotely** from the **Actions** menu.
- 3 In the Monitor Remote Object dialog, select the Endpoint Operations Management agent that will remotely monitor the object from the **Monitored From** menu.
- 4 Select the method with which the remote object will be monitored from the **Check Method** menu.

The relevant parameters for the selected object type appear.

- 5 Enter values for all of the configuration options and click **OK**.

### HTTP Configuration Options

Here are the options in the configuration schema for the HTTP resource.

For the HTTP resource, the `netservices` plug-in descriptor default values are:

- `port`: 80
- `sslport`: 443

#### HTTP Configuration Options

**Table 1-4. ssl Option**

Option Information	Value
Description	Use ssl
Default	false
Optional	true
Type	boolean

Option Information	Value
Notes	N/A
Parent Schema	ssl

**Table 1-5. hostname Option**

Option Information	Value
Description	Hostname
Default	localhost
Optional	false
Type	N/A
Notes	The hostname of system that hosts the service to monitor. For example: mysite.com
Parent Schema	sockaddr

**Table 1-6. port Option**

Option Information	Value
Description	Port
Default	A default value for port is usually set for each type of network service by properties in the net services plug-in descriptor.
Optional	false
Type	N/A
Notes	The port on which the service listens.
Parent Schema	sockaddr

**Table 1-7. sotimeout Option**

Option Information	Value
Description	Socket Timeout (in seconds)
Default	10
Optional	true
Type	int
Notes	The maximum length of time the agent waits for a response to a request to the remote service.
Parent Schema	sockaddr

**Table 1-8. path Option**

Option Information	Value
Description	Path
Default	/
Optional	false
Type	N/A
Notes	Enter a value to monitor a specific page or file on the site. for example: /Support.html.
Parent Schema	url

**Table 1-9. method Option**

Option Information	Value
Description	Request Method
Default	HEAD
Optional	false
Type	enum
Notes	Method for checking availability. Permitted values: HEAD, GET HEAD results in less network traffic. Use GET to return the body of the request response to specify a pattern to match in the response.
Parent Schema	http

**Table 1-10. hostheader Option**

Option Information	Value
Description	Host Header
Default	none
Optional	true
Type	N/A
Notes	Use this option to set a Host HTTP header in the request. This is useful if you use name-based virtual hosting. Specify the host name of the Vhost's host, for example, blog.mypost.com.
Parent Schema	http

**Table 1-11. follow Option**

Option Information	Value
Description	Follow Redirects
Default	enabled

Option Information	Value
Optional	true
Type	boolean
Notes	Enable if the HTTP request that is generated will be re-directed. This is important, because an HTTP server returns a different code for a redirect and vRealize Operations Manager determines that the HTTP service check is unavailable if it is a redirect, unless this redirect configuration is set.
Parent Schema	http

**Table 1-12. pattern Option**

Option Information	Value
Description	Response Match (substring or regex)
Default	none
Optional	true
Type	N/A
Notes	Specify a pattern or substring for vRealize Operations Manager to attempt to match against the content in the HTTP response. This enables you to check that in addition to being available, the resource is serving the content you expect.
Parent Schema	http

**Table 1-13. proxy Option**

Option Information	Value
Description	Proxy Connection
Default	none
Optional	true
Type	N/A
Notes	If the connection to the HTTP service goes through a proxy server, supply the hostname and port for the proxy server. For example, proxy.myco.com:3128.
Parent Schema	http

**Table 1-14. requestparams Option**

Option Information	Value
Description	Request arguments. For example, arg0=val0, arg1=val1, and so on.
Default	N/A
Optional	true
Type	string

Option Information	Value
Notes	Request parameters added to the URL to be tested.
Parent Schema	http

**Table 1-15. Credential Option**

Option Information	Value
Description	Username
Default	N/A
Optional	true
Type	N/A
Notes	Supply the user name if the target site is password-protected.
Parent Schema	credentials

**ICMP Configuration Options**

Here are the options in the configuration schema for the ICMP resource.

ICMP configuration is not supported in Windows environments. When attempting to run an ICMP check for remote monitoring from an Agent running on a Windows platform, no data is returned.

**Table 1-16. hostname Option**

Option Information	Value
Description	Hostname
Default	localhost
Optional	N/A
Type	N/A
Notes	The hostname of system that hosts the object to monitor. For example: mysite.com
Parent Schema	netservices plug-in descriptor

**Table 1-17. sotimeout Option**

Option Information	Value
Description	Socket Timeout (in seconds)
Default	10
Optional	N/A
Type	int
Notes	The maximum period of time the agent waits for a response to a request to the remote service.
Parent Schema	netservices plug-in descriptor

**TCP Configuration Options**

Here are the options in the configuration schema to enable TCP checking.

**Table 1-18. port Option**

Option Information	Value
Description	Port
Default	A default value for port is usually set for each type of network service by properties in the netsservices plug-in descriptor.
Optional	false
Type	N/A
Notes	The port on which the service listens.
Parent Schema	sockaddr

**Table 1-19. hostname Option**

Option Information	Value
Description	Hostname
Default	localhost
Optional	N/A
Type	N/A
Notes	The hostname of system that hosts the object to monitor. For example: mysite.com
Parent Schema	netsservices plug-in descriptor

Make sure you use the IP address of the machine on which the remote check is to run, not the host name.

**Table 1-20. sotimeout Option**

Option Information	Value
Description	Socket Timeout (in seconds)
Default	10
Optional	N/A
Type	int
Notes	The maximum amount of time the agent waits for a response to a request to the remote service.
Parent Schema	netsservices plug-in descriptor

## Working with Agent Plug-ins

Endpoint Operations Management agents include plug-ins that determine which objects to monitor, how they should be monitored, which metrics to collect, and so on. Some plug-ins are included in the default Endpoint Operations Management agent installation, and other plug-ins might be added as part of any management pack solution that you install to extend the vRealize Operations Manager monitoring process.

You can use the **Plug-in** tab in the Content view to disable or enable the agent plug-ins that are deployed in your environment as part of a solution installation. For example, you might want to temporarily disable a plug-in so that you can analyze the implication of that plug-in on a monitored virtual machine.

All the default plug-ins and the plug-ins that are deployed when you installed one or more solutions are listed alphabetically on the tab.

You must have Manage Plug-ins permissions to enable and disable plug-ins.

When you disable a plug-in, it is removed from all the agents on which it has existed, and the agent no longer collects the metrics and other data related to that plug-in. The plug-in is marked as disabled on the vRealize Operations Manager server.

You cannot disable the default plug-ins that are installed during the vRealize Operations Manager installation.

You use the action menu that appears when you click the gear wheel icon to disable or enable plug-ins.

Before you deploy a new version of a plug-in, you must implement a shut down method. If you do not implement a shut down method, the existing plug-in version does not shut down so that a new instance is created and allocated resources such as static threads are not released. Implement a shut down method for these plug-ins.

- Plug-ins that use third-party libraries
- Plug-ins that use native libraries
- Plug-ins that use connection pools
- Plug-ins that might lock files, which cause issues on Windows operating systems

It is good practice that plug-ins do not use threads, third-party libraries, or static collection.

### Configuring Plug-in Loading

At startup, an Endpoint Operations Management agent loads all the plug-ins in the `AgentHome/bundles/agent-x.y.z-nnnn/pdk/plugins` directory. You can configure properties in the `agent.properties` file to reduce an agent's memory footprint by configuring it to load only the plug-ins that you use.

Plug-ins are deployed to all agents when a solution is installed. You might want to use the properties described here in a situation in which you need to remove one or more plug-ins from a specific machine. You can either specify a list of plug-ins to exclude, or configure a list of plug-ins to load.

#### **plugins.exclude**

Use this property to specify the plug-ins that the Endpoint Operations Management agent must not load at startup.

You supply a comma-separated list of plugins to exclude. For example, `plugins.exclude=jboss,apache,mysql`.

#### **plugins.include**

Use this property to specify the plug-ins that the Endpoint Operations Management agent must load at startup.

You supply a comma-separated list of plugins to include. For example, `plugins.include=weblogic,apache`.

## Understanding the Unsynchronized Agents Group

An unsynchronized agent is an agent that is not synchronized with the vRealize Operations Manager server in terms of its plug-ins. The agent might be missing plug-ins that are registered on the server, include plug-ins that are not registered on the server, or include plug-ins that have a different version to that registered on the server.

Each agent must be synchronized with the vRealize Operations Manager server. During the time that an agent is not synchronized with the server, it appears in the Unsynchronized Agents list. The list is located in the vRealize Operations Manager user interface on the **Groups** tab in the Environment view.

The first time an agent is started, a status message is sent to the server. The server compares the status sent by the agent with that on the server. The server sends commands to the agent to synchronize, download or delete plug-ins, as required by the differences that it detects.

When a plug-in is deployed, disabled, or enabled as part of a management pack solution update, the vRealize Operations Manager server detects that change and sends a new command to the agents so that synchronization occurs.

Commonly, multiple agents are affected at the same time when a plug-in is deployed, disabled or enabled. All agents have an equal need to be updated so, to avoid overloading the server and creating performance issues that might occur if many agents were all synchronized at the same time, synchronization is performed in batches and is staggered in one-minute periods. You will notice that the list of unsynchronized agents decrements over time.

## Configuring Agent Logging

You can configure the name, location, and logging level for Endpoint Operations Management agent logs. You can also redirect system messages to the agent log, and configure the debug log level for an agent subsystem.

### Agent Log Files

The Endpoint Operations Management agent log files are stored in the `AgentHome/Log` directory.

Agent log files include the following:

#### **agent.log**

#### **agent.operations.log**

This log is applicable to Windows-based agents only.

This is an audit log that records the commands that were run on the agent, together with the parameters that the agent used to action them.

#### **wrapper.log**

The Java service wrapper-based agent launcher writes messages to the `wrapper.log` file. For a non-JRE agent, this file is located in `agentHome/wrapper/sbin`.

In the event that the value was changed for the `agent.logDir` property, the file is also located in `agentHome/wrapper/sbin`.

## Configuring the Agent Log Name or Location

Use these properties to change the name or location of the agent log file.

### **agent.logDir**

You can add this property to the `agent.properties` file to specify the directory where the Endpoint Operations Management agent will write its log file. If you do not specify a fully qualified path, `agent.logDir` is evaluated relative to the agent installation directory.

This property does not exist in the `agent.properties` file unless you explicitly add it. The default behavior is equivalent to the `agent.logDir=log` setting, resulting in the agent log file being written to the `AgentHome/log` directory.

To change the location for the agent log file, add `agent.logDir` to the `agent.properties` file and enter a path relative to the agent installation directory, or a fully qualified path.

The name of the agent log file is configured with the `agent.logFile` property.

### **agent.logFile**

This property specifies the path and name of the agent log file.

In the `agent.properties` file, the default setting for the `agent.logFile` property is made up of a variable and a string, `agent.logFile=${agent.logDir}\agent.logDir`.

- `agent.logDir` is a variable that supplies the value of an identically named agent property. By default, the value of `agent.logDir` is `log`, interpreted relative to the agent installation directory.
- `agent.log` is the name for the agent log file.

By default, the agent log file is named `agent.log` and is written to the `AgentHome/log` directory.

To configure the agent to log to a different directory, you must explicitly add the `agent.logDir` property to the `agent.properties` file.

## Configuring the Agent Logging Level

Use this property to control the severity level of messages that the Endpoint Operations Management agent writes to the agent log file.

### **agent.logLevel**

This property specifies the level of detail of the messages that the Endpoint Operations Management agent writes to the log file.

Setting the `agent.logLevel` property value to `DEBUG` level is not advised. This level of logging across all subsystems imposes overhead, and can also cause the log file to roll over so frequently that log messages of interest are lost. It is preferable to configure debug level logging only at the subsystem level.

The changes that you make to this property become effective approximately five minutes after you save the properties file. It is not necessary to restart the agent to initiate the change.

## Redirecting System Messages to the Agent Log

You can use these properties to redirect system-generated messages to the Endpoint Operations Management agent log file.

### **agent.logLevel.SystemErr**

This property redirects `System.err` to `agent.log`. Commenting out this setting causes `System.err` to be directed to `agent.log.startup`.

The default value is `ERROR`.

### **agent.logLevel.SystemOut**

This property redirects `System.out` to `agent.log`. Commenting out this setting causes `System.out` to be directed to `agent.log.startup`.

The default value is `INFO`.

## Configuring the Debug Level for an Agent Subsystem

For troubleshooting purposes, you can increase the logging level for an individual agent subsystem.

To increase the logging level for an individual agent subsystem, uncomment the appropriate line in the section of the `agent.properties` file that is labelled `Agent Subsystems: Uncomment individual subsystems` to see debug messages.

### Agent log4j Properties

This is the `log4j` properties in the `agent.properties` file.

```
log4j.rootLogger=${agent.logLevel}, R

log4j.appender.R.File=${agent.logFile}
log4j.appender.R.MaxBackupIndex=1
log4j.appender.R.MaxFileSize=5000KB
log4j.appender.R.layout.ConversionPattern=%d{dd-MM-yyyy HH:mm:ss,SSS z} %-5p [%t] [%c{1}@%L] %m%n
log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R=org.apache.log4j.RollingFileAppender

##
## Disable overly verbose logging
##
log4j.logger.org.apache.http=ERROR
log4j.logger.org.springframework.web.client.RestTemplate=ERROR
log4j.logger.org.hyperic.hq.measurement.agent.server.SenderThread=INFO
log4j.logger.org.hyperic.hq.agent.server.AgentDListProvider=INFO
log4j.logger.org.hyperic.hq.agent.server.MeasurementSchedule=INFO
log4j.logger.org.hyperic.util.units=INFO
log4j.logger.org.hyperic.hq.product.pluginxml=INFO

# Only log errors from naming context
log4j.category.org.jnp.interfaces.NamingContext=ERROR
log4j.category.org.apache.axis=ERROR

#Agent Subsystems: Uncomment individual subsystems to see debug messages.
#-----
```

```

#log4j.logger.org.hyperic.hq.autoinventory=DEBUG
#log4j.logger.org.hyperic.hq.livedata=DEBUG
#log4j.logger.org.hyperic.hq.measurement=DEBUG
#log4j.logger.org.hyperic.hq.control=DEBUG

#Agent Plugin Implementations
#log4j.logger.org.hyperic.hq.product=DEBUG

#Server Communication
#log4j.logger.org.hyperic.hq.bizapp.client.AgentCallbackClient=DEBUG

#Server Realtime commands dispatcher
#log4j.logger.org.hyperic.hq.agent.server.CommandDispatcher=DEBUG

#Agent Configuration parser
#log4j.logger.org.hyperic.hq.agent.AgentConfig=DEBUG

#Agent plugins loader
#log4j.logger.org.hyperic.util.PluginLoader=DEBUG

#Agent Metrics Scheduler (Scheduling tasks definitions & executions)
#log4j.logger.org.hyperic.hq.agent.server.session.AgentSynchronizer.SchedulerThread=DEBUG

#Agent Plugin Managers
#log4j.logger.org.hyperic.hq.product.MeasurementPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.AutoinventoryPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.ConfigTrackPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.LogTrackPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.LiveDataPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.ControlPluginManager=DEBUG

```

## Log Insight

When vRealize Operations Manager is integrated with Log Insight, you can view the Log Insight page, Log Insight dashboard, and the Logs tab. You can collect and analyze log feeds. You can filter and search for log messages. You can also dynamically extract fields from log messages based on customized queries.

### Log Insight Page

When vRealize Operations Manager is integrated with vRealize Log Insight, you can search and filter log events. From the Interactive Analytics tab in the Log Insight page, you can create queries to extract events based on timestamp, text, source, and fields in log events . vRealize Log Insight presents charts of the query results.

To access the Log Insight page from vRealize Operations Manager, you must either:

- Configure the vRealize Log Insight adapter from the vRealize Operations Manager interface, or
- Configure vRealize Operations Manager in vRealize Log Insight.

For more information about configuring, see [Configuring vRealize Log Insight with vRealize Operations Manager](#).

For information about vRealize Log Insight interactive analytics, see the [vRealize Log Insight documentation](#).

## Logs Tab

When vRealize Operations Manager is integrated with vRealize Log Insight, you can view the logs for a selected object from the Logs tab. You can troubleshoot a problem in your environment by correlating the information in the logs with the metrics. You can then most likely determine the root cause of the problem.

### How the Logs Tab Works

By default, the Logs tab displays different event types for the last hour. For vSphere objects, the logs are filtered to show the event types for the specific object you select. For more information on the different filtering and querying capabilities, see the [vRealize Log Insight documentation](#).

### Where You Find the Logs Tab

From the left pane, select **Environment** and then select an inventory object. Click the **Logs** tab. To view the Logs tab, you have to configure vRealize Operations Manager in vRealize Log Insight. For more information, see [Configuring vRealize Log Insight with vRealize Operations Manager](#).

## Configuring vRealize Log Insight with vRealize Operations Manager

To use the Log Insight page, Log Insight dashboard, and Logs tab in vRealize Operations Manager, you must configure vRealize Log Insight with vRealize Operations Manager.

### Configuring the vRealize Log Insight Adapter in vRealize Operations Manager

To access the Log Insight page and Log Insight dashboard from vRealize Operations Manager, you must configure the vRealize Log Insight adapter in vRealize Operations Manager.

vRealize Operations Manager accesses the first instance of the vRealize Log Insight adapter that is configured.

#### Prerequisites

- Verify that vRealize Log Insight and vRealize Operations Manager are installed.
- Verify that you know the IP address, user name, and password of the vRealize Log Insight instance you have installed.

#### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon and then click **Solutions**.
- 2 From the Solutions page, click VMware vRealize Log Insight.
- 3 Click the **Configure** icon. You see the Manage Solution-VMware vRealize Log Insight dialog box.
- 4 In the Manage Solutions dialog box perform the following steps:
  - Enter a name in the **Display Name** text box.

- Enter the IP address in the **Log Insight server** text box of the vRealize Log Insight you have installed and want to integrate with.
  - Click **Test Connection** to verify that the connection is successful.
  - Click **Save Settings**.
  - Click **Close**.
- 5 From the vRealize Operations Manager Home page, click the **Log Insight** icon. If you see a statement at the bottom of the page, click the link and accept the certificate exception in vRealize Log Insight or contact your IT support for more information.
  - 6 From the vRealize Operations Manager Home page, click the **Log Insight** icon and enter the user name and password of the vRealize Log Insight instance you have installed.

## Configuring vRealize Operations Manager in vRealize Log Insight

You configure vRealize Operations Manager in vRealize Log Insight in the following scenarios:

- To access the Logs tab in vRealize Operations Manager.
- To access the Log Insight dashboard and Log Insight page from vRealize Operations Manager.

### Prerequisites

- Verify that vRealize Log Insight and vRealize Operations Manager are installed.
- Verify that you know the IP address, hostname, and password of the vRealize Operations Manager instance you want to integrate with.

### Procedure

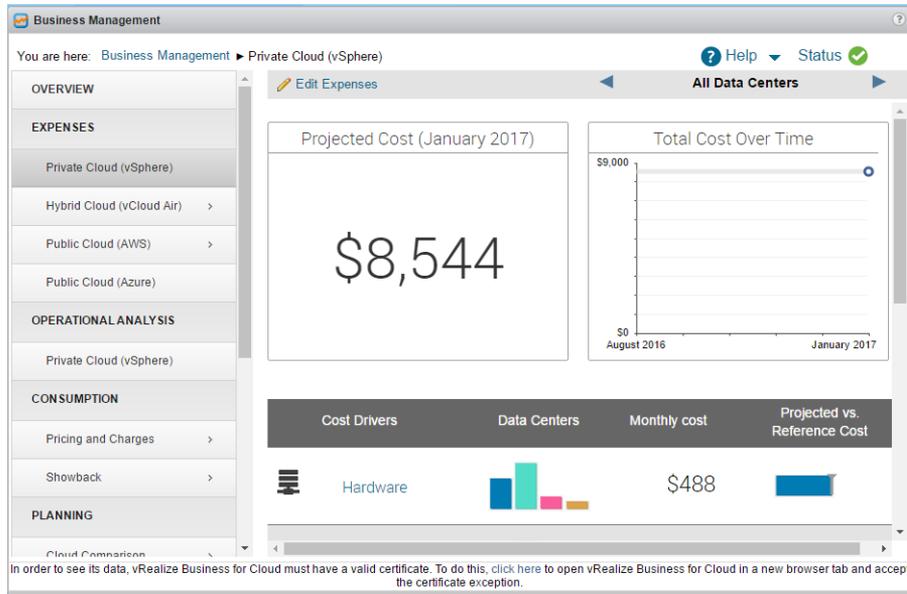
- 1 From the Administration page of vRealize Log Insight, click the **vRealize Operations** icon from the left pane. You see the vRealize Operations Integration pane.
- 2 In the **Hostname** and **Username** text boxes, enter the IP address and hostname of the vRealize Operations Manager instance you want to integrate with.
- 3 In the **Password** text box, select **Update Password** and enter the password of the vRealize Operations Manager instance you want to integrate with.
- 4 Select the **Enable launch in context** option.
- 5 Click **Test Connection** to verify that the connection is successful.
- 6 Click **Save**.

You can now view the log details for an object in vRealize Operations Manager.

## Business Management

When vRealize Operations Manager is integrated with vRealize Business for Cloud, you can display infrastructure performance and cost information in the Business Management page and the Business Management dashboard.

To display infrastructure performance and cost information, you must configure the vRealize Business for Cloud adapter. For information about configuring this adapter, refer to [Configure vRealize Business for Cloud Adapter](#).



## Configure vRealize Business for Cloud Adapter

Integrate VMware vRealize Business for Cloud with vRealize Operations Manager to view your infrastructure performance, cost information, and also troubleshooting tips.

You can connect vRealize Operations Manager to a single instance of vRealize Business for Cloud.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click **Administration > Solutions**.
- 2 Select **VMware vRealize Business for Cloud**, and click the **Configure** icon.
- 3 Enter a name for the adapter instance.
- 4 In the **vRealize Business for Cloud Server** field, enter the IP address of the vRealize Business for Cloud server to which you want to connect.
- 5 Click **Test Connection** to verify that the connection is successful.
- 6 Click **Advanced Settings**, and in the **Collectors/Groups** field, specify which vRealize Operations Manager collector is used to manage the adapter process.

If you have one adapter instance, select **Default collector group**. If you have multiple collectors in your environment, and you want to distribute the workload to optimize performance, select the collector to manage the adapter processes for this instance.

- 7 Click **Save Settings** to complete configuration of the adapter.

## What to do next

View cost information in the [Business Management Dashboard](#), or the [Business Management](#) page.

# Installing Optional Solutions in vRealize Operations Manager

You can extend the monitoring capabilities of vRealize Operations Manager by installing optional solutions from VMware or third parties.

VMware solutions include adapters for Storage Devices, Log Insight, NSX for vSphere, Network Devices, and VCM. Third-party solutions include AWS, SCOM, EMC Smarts, and many others. To download software and documentation for optional solutions, visit the [VMware Solution Exchange](#).

Solutions can include dashboards, reports, alerts and other content, and adapters. Adapters are how vRealize Operations Manager manages communication and integration with other products, applications, and functions. When a management pack is installed and the solution adapters are configured, you can use the vRealize Operations Manager analytics and alerting tools to manage the objects in your environment.

If you upgrade from an earlier version of vRealize Operations Manager, your management pack files are copied to the `/usr/lib/vmware-vcops/user/plugins/.backup` file in a folder with a date and time as the folder name. Before migrating your data to your new vRealize Operations Manager instance, you must configure the new adapters in the **Administration > Solutions** workspace. If you have customized the adapter, your adapter customizations are not included in the migration, and you must reconfigure them.

If you update a management pack in vRealize Operations Manager to a newer version, and you have customized the adapter, your adapter customizations are not included in the upgrade, and you must reconfigure them.

## Managing Solution Credentials

Credentials are the user accounts that vRealize Operations Manager uses to enable one or more solutions and associated adapters, and to establish communication with the target data sources. The credentials are supplied when you configure each adapter. You use the credential option to add or modify the settings outside the adapter configuration process, accommodating changes to your environment.

If you are modifying existing credentials, for example, to accommodate changes based on your password policy, the adapters configured with these credentials begin using the new user name and password for communication between the vRealize Operations Manager and the target system.

Another use of credential management is to remove misconfigured credentials. If you delete valid credentials that were in active use by an adapter, you disable the communication between the two systems.

If you need to change the configured credential to accommodate changes in your environment, you can edit settings, for example, name, user name and password, or pass code and key phrase, without being required to configure a new adapter instance for the target system. You can edit credential settings by clicking **Administration** and then clicking **Credentials**.

Any adapter credential you add are shared with other adapter administrators and vRealize Operations Manager collector hosts. Other administrators might use these credential to configure a new adapter instance or to move an adapter instance to a new host.

## Manage Credentials

To configure or reconfigure credentials that you use to enable an adapter instance, you must provide the collection configuration settings, for example, user name and password, that are valid on the target system. You can also modify the connection settings for an existing credential instance.

### Where You Find Manage Credentials

In the left pane, click the **Administration** icon and click **Credentials**. Click the plus sign to add a new credential or the pencil to edit the selected credential.

### Manage Credentials Options

The Manage Credentials dialog box is used to add new or modifies existing adapter credentials. The dialog box varies depending on the type of adapter and whether you are adding or editing. The following options describe the basic options. Depending on the solution, the options other than the basic ones vary.

**Caution** Any adapter credentials you add are shared with other adapter administrators and vRealize Operations Manager collector hosts. Other administrators might use these credentials to configure a new adapter instance or to move an adapter instance to a new host.

**Table 1-21. Manage Credential Add or Edit Options**

Option	Description
Adapter Type	Adapter type for which you are configuring the credentials.
Credential Kind	Credentials associated with the adapter. The combination of adapter and credential type affects the additional configuration options.
Credential Name	Descriptive name by which you are managing the credentials.
User Name	User account credentials that are used in the adapter configuration to connect vRealize Operations Manager to the target system.
Password	Password for the provided credentials.

## Managing Collector Groups

vRealize Operations Manager uses collectors to manage adapter processes such as gathering metrics from objects. You can select a collector or a collector group when configuring an adapter instance.

If there are remote collectors in your environment, you can create a new collector group, and add remote collectors to the group. When you assign an adapter to a collector group, the adapter can use any collector in the group. Use collector groups to achieve adapter resiliency in cases where the collector experiences network interruption or becomes unavailable. If this occurs, and the collector is part of a group, the total workload is redistributed among all the collectors in the group, reducing the workload on each collector.

# Configuring Alerts and Actions

In VMware vRealize Operations Manager, alerts and actions play key roles in monitoring the objects.

This chapter includes the following topics:

- [Types of Alerts](#)
- [Configuring Alerts](#)
- [Configuring Actions](#)

## Types of Alerts

Different types of alerts are triggered on a certain object.

The alerts are of three types:

- Health Alerts
- Risk Alerts
- Efficiency Alerts

## Configuring Alerts

Whenever there is a problem in the environment, the alerts are generated. You can create the alert definitions so that the generated alerts tell you about the problems in the monitored environment.

## Defining Alerts in vRealize Operations Manager

An alert definition comprises one or more symptom definitions, and the alert definition is associated with a set of recommendations and actions that help you resolve the problem. Alert definitions include triggering symptom definitions and actionable recommendations. You create the alert definitions so that the generated alerts tell you about problems in the monitored environment. You can then respond to the alerts with effective solutions that are provided in the recommendations.

Predefined alerts are provided in vRealize Operations Manager as part of your configured adapters. You can add or modify alert definitions to reflect the needs of your environment.



Create Alert Definitions for vRealize Operations Manager  
([http://link.brightcove.com/services/player/bcpid2296383276001?  
bctid=ref:video\\_create\\_alerts\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_create_alerts_vrom))

## Symptoms in Alert Definitions

Symptom definitions evaluate conditions in your environment that, if the conditions become true, trigger a symptom and can result in a generated alert. You can add symptom definitions that are based on metrics or super metrics, properties, message events, fault events, or metric events. You can create a symptom definition as you create an alert definition or as an individual item in the appropriate symptom definition list.

When you add a symptom definition to an alert definition, it becomes a part of a symptom set. A symptom set is the combination of the defined symptom with the argument that determines when the symptom condition becomes true.

A symptom set combines one or more symptom definitions by applying an Any or All condition, and allows you to choose the presence or absence of a particular symptom. If the symptom set pertains to related objects rather than to Self, you can apply a population clause to identify a percentage or a specific count of related objects that exhibit the included symptom definitions.

An alert definition comprises one or more symptom sets. If an alert definition requires all of the symptom sets to be triggered before generating an alert, and only one symptom set is triggered, an alert is not generated. If the alert definition requires only one of several symptom sets to be triggered, then the alert is generated even though the other symptom sets were not triggered.

## Recommendations in Alert Definitions

Recommendations are the remediation options that you provide to your users to resolve the problems that the generated alert indicates.

When you add an alert definition that indicates a problem with objects in your monitored environment, add a relevant recommendation. Recommendations can be instructions to your users, links to other information or instruction sources, or vRealize Operations Manager actions that run on the target systems.

## Modifying Alert Definitions

If you modify the alert impact type of an alert definition, any alerts that are already generated will have the previous impact level. Any new alerts will be at the new impact level. If you want to reset all the generated alerts to the new level, cancel the old alerts. If they are generated after cancellation, they will have the new impact level.

## Defining Symptoms for Alerts

Symptoms are conditions that indicate problems in your environment. You define symptoms that you add to alert definitions so that you know when a problem occurs with your monitored objects.

As data is collected from your monitored objects, the data is compared to the defined symptom condition. If the condition is true, then the symptom is triggered.

You can define symptoms based on metrics and super metrics, properties, message events, fault events, and metric events.

Defined symptoms in your environment are managed in the Symptom Definitions. When the symptoms that are added to an alert definition are triggered, they contribute to a generated alert. Symptoms that are not added to an alert definition are still evaluated and if the condition is evaluated as true, appear on the **Alert Details Symptom** tab on the **Troubleshooting** tab.

## Define Symptoms to Cover All Possible Severities and Conditions

Use a series of symptoms to describe incremental levels of concern. For example, `Volume nearing capacity limit` might have a severity value of `Warning` while `Volume reached capacity limit` might have a severity level of `Critical`. The first symptom is not an immediate threat. The second symptom is an immediate threat.

## About Metrics and Super Metrics Symptoms

Metric and super metric symptoms are based on the operational or performance values that vRealize Operations Manager collects from target objects in your environment. You can configure the symptoms to evaluate static thresholds or dynamic thresholds.

You define symptoms based on metrics so that you can create alert definitions that let you know when the performance of an object in your environment is adversely affected.

### Static Thresholds

Metric symptoms that are based on a static threshold compare the currently collected metric value against the fixed value you configure in the symptom definition.

For example, you can configure a static metric symptom where, when the virtual machine CPU workload is greater than 90, a critical symptom is triggered.

### Dynamic Thresholds

Metric symptoms that are based on dynamic thresholds compare the currently collected metric value against the trend identified by vRealize Operations Manager, evaluating whether the current value is above, below, or generally outside the trend.

For example, you can configure a dynamic metric symptom where, when the virtual machine CPU workload is above the trended normal value, a critical symptom is triggered.

## Property Symptoms

Property symptoms are based on the configuration properties that vRealize Operations Manager collects from the target objects in your environment.

You define symptoms based on properties so that you can create alert definitions that let you know when changes to properties on your monitored objects can affect the behavior of the objects in your environment.

## Message Event Symptoms

Message event symptoms are based on events received as messages from a component of vRealize Operations Manager or from an external monitored system through the system's REST API. You define

symptoms based on message events to include in alert definitions that use these symptoms. When the configured symptom condition is true, the symptom is triggered.

The adapters for the external monitored systems and the REST API are inbound channels for collecting events from external sources. Adapters and the REST server both run in the vRealize Operations Manager system. The external system sends the messages, and vRealize Operations Manager collects them.

You can create message event symptoms for the supported event types. The following list is of supported event types with example events.

- System Performance Degradation. This message event type corresponds to the `EVENT_CLASS_SYSTEM` and `EVENT_SUBCLASS_PERFORM_DEGRADATION` type and subtype in the vRealize Operations Manager API SDK.
- Change. The VMware adapter sends a change event when the CPU limit for a virtual machine is changed from unlimited to 2 GHz. You can create a symptom to detect CPU contention issues as a result of this configuration change. This message event type corresponds to the `EVENT_CLASS_CHANGE` and `EVENT_SUBCLASS_CHANGE` type and subtype in the vRealize Operations Manager API SDK.
- Environment Down. The vRealize Operations Manager adapter sends an environment down event when the collector component is not communicating with the other components. You can create a symptom that is used for internal health monitoring. This message event type corresponds to the `EVENT_CLASS_ENVIRONMENT` and `EVENT_SUBCLASS_DOWN` type and subtype in the vRealize Operations Manager API SDK.
- Notification. This message event type corresponds to the `EVENT_CLASS_NOTIFICATION` and `EVENT_SUBCLASS_EXTEVENT` type and subtype in the vRealize Operations Manager API SDK.

## Fault Symptoms

Fault symptoms are based on events published by monitored systems. vRealize Operations Manager correlates a subset of these events and delivers them as faults. Faults are intended to signify events in the monitored systems that affect the availability of objects in your environment. You define symptoms based on faults to include in alert definitions that use these symptoms. When the configured symptom condition is true, the symptom is triggered.

You can create fault symptoms for the supported published faults. Some object types have multiple fault definitions from which to choose, while others have no fault definitions.

If the adapter published fault definitions for an object type, you can select one or more fault events for a given fault while you define the symptom. The symptom is triggered if the fault is active because of any of the chosen events. If you do not select a fault event, the symptom is triggered if the fault is active because of a fault event.

## Metric Event Symptoms

Metric event symptoms are based on events communicated from a monitored system where the selected metric violates a threshold in a specified manner. The external system manages the threshold, not vRealize Operations Manager.

Metric event symptoms are based on conditions reported for selected metrics by an external monitored system, as compared to metric symptoms, which are based on thresholds that vRealize Operations Manager is actively monitoring.

The metric event thresholds, which determine whether the metric is above, below, equal to, or not equal to the threshold set on the monitored system, represent the type and subtype combination that is specified in the incoming metric event.

- Above Threshold. Corresponds to type and subtype constants `EVENT_CLASS_HT` and `EVENT_SUBCLASS_ABOVE` defined in the vRealize Operations Manager API SDK.
- Below Threshold. Corresponds to type and subtype constants `EVENT_CLASS_HT` and `EVENT_SUBCLASS_BELOW` defined in the vRealize Operations Manager API SDK.
- Equal Threshold. Corresponds to type and subtype constants `EVENT_CLASS_HT` and `EVENT_SUBCLASS_EQUAL` defined in the vRealize Operations Manager API SDK.
- Not Equal Threshold. Corresponds to type and subtype constants `EVENT_CLASS_HT` and `EVENT_SUBCLASS_NOT_EQUAL` defined in the vRealize Operations Manager API SDK.

## Understanding Negative Symptoms for vRealize Operations Manager Alerts

Alert symptoms are conditions that indicate problems in your environment. When you define an alert, you include symptoms that generate the alert when they become true in your environment. Negative symptoms are based on the absence of the symptom condition. If the symptom is not true, the symptom is triggered.

To use the absence of the symptom condition in an alert definition, you negate the symptom in the symptom set.

All defined symptoms have a configured criticality. However, if you negate a symptom in an alert definition, it does not have an associated criticality when the alert is generated.

All symptom definitions have a configured criticality. If the symptom is triggered because the condition is true, the symptom criticality will be the same as the configured criticality. However, if you negate a symptom in an alert definition and the negation is true, it does not have an associated criticality.

When negative symptoms are triggered and an alert is generated, the effect on the criticality of the alert depends on how the alert definition is configured.

The following table provides examples of the effect negative symptoms have on generated alerts.

**Table 2-1. Negative Symptoms Effect on Generated Alert Criticality**

<b>Alert Definition Criticality</b>	<b>Negative Symptom Configured Criticality</b>	<b>Standard Symptom Configured Criticality</b>	<b>Alert Criticality When Triggered</b>
Warning	One Critical Symptom	One Immediate Symptom	Warning. The alert criticality is based on the defined alert criticality.
Symptom Based	One Critical Symptom	One Warning Symptom	Warning. The negative symptom has no associated criticality and the criticality of the standard symptom determines the criticality of the generated alert.
Symptom Based	One Critical Symptom	No standard symptom included	Info. Because an alert must have a criticality and the negative alert does not have an associated criticality, the generated alert has a criticality of Info, which is the lowest possible criticality level.

## Defining Recommendations for Alert Definitions

Recommendations are instructions to your users who are responsible for responding to alerts. You add recommendations to vRealize Operations Manager alerts so that your users can maintain the objects in your environment at the required levels of performance.

Recommendations provide your network engineers or virtual infrastructure administrators with information to resolve alerts.

Depending on the knowledge level of your users, you can provide more or less information, including the following options, in any combination.

- One line of instruction.
- Steps to resolve the alert on the target object.
- Hyperlink to a Web site, runbook, wiki, or other source.
- Action that makes a change on the target object.

When you define an alert, provide as many relevant action recommendations as possible. If more than one recommendation is available, arrange them in priority order so that the solution with the lowest effect and highest effectiveness is listed first. If no action recommendation is available, add text recommendations. Be as precise as possible when describing what the administrator should do to fix the alert.

## Create a New Alert Definition

Based on the root cause of the problem, and the solutions that you used to fix the problem, you can create a new alert definition for vRealize Operations Manager to alert you. When the alert is triggered on

your host system, vRealize Operations Manager alerts you and provides recommendations on how to solve the problem.

To alert you before your host systems experience critical capacity problems, and have vRealize Operations Manager notify you of problems in advance, you create alert definitions, and add symptom definitions to the alert definition.

### Procedure

1 In the left pane, click **Content > Alert Definitions**.

2 Enter **capacity** in the search text box.

Review the available list of capacity alert definitions. If a capacity alert definition does not exist for host systems, you can create one.

3 Click the plus sign to create a new capacity alert definition for your host systems.

a In the alert definition workspace, for the Name and Description, enter **Hosts – Alert on Capacity Exceeded**.

b For the Base Object Type, select **vCenter Adapter > Host System**

c For the Alert Impact, select the following options.

Option	Selection
Impact	Select <b>Risk</b> .
Criticality	Select <b>Immediate</b> .
Alert Type and Subtype	Select <b>Application : Capacity</b> .
Wait Cycle	Select <b>1</b> .
Cancel Cycle	Select <b>1</b> .

d For Add Symptom Definitions, select the following options.

Option	Selection
Defined On	Select <b>Self</b> .
Symptom Definition Type	Select <b>Metric / Supermetric</b> .
Quick filter (Name)	Enter <b>capacity</b> .

e From the Symptom Definition list, click **Host System Capacity Remaining is moderately low** and drag it to the right pane.

In the Symptoms pane, make sure that the Base object exhibits criteria is set to **All** by default.

f For Add Recommendations, enter **virtual machine** in the quick filter text box.

g Click **Review the symptoms listed and remove the number of vCPUs from the virtual machine as recommended by the system**, and drag it to the recommendations area in the right pane.

This recommendation is set to Priority 1.

#### 4 Click **Save** to save the alert definition.

Your new alert appears in the list of alert definitions.

You have added an alert definition to have vRealize Operations Manager alert you when the capacity of your host systems begins to run out.

## Alert Definition Best Practices

As you create alert definitions for your environment, apply consistent best practices so that you optimize alert behavior for your monitored objects.

### Alert Definitions Naming and Description

The alert definition name is the short name that appears in the following places:

- In data grids when alerts are generated
- In outbound alert notifications, including the email notifications that are sent when outbound alerts and notifications are configured in your environment

Ensure that you provide an informative name that clearly states the reported problem. Your users can evaluate alerts based on the alert definition name.

The alert definition description is the text that appears in the alert definition details and the outbound alerts. Ensure that you provide a useful description that helps your users understand the problem that generated the alert.

### Wait and Cancel Cycle

The wait cycle setting helps you adjust for sensitivity in your environment. The wait cycle for the alert definition goes into effect after the wait cycle for the symptom definition results in a triggered symptom. In most alert definitions you configure the sensitivity at the symptom level and configure the wait cycle of alert definition to 1. This configuration ensures that the alert is immediately generated after all of the symptoms are triggered at the desired symptom sensitivity level.

The cancel cycle setting helps you adjust for sensitivity in your environment. The cancel cycle for the alert definition goes into effect after the cancel cycle for the symptom definition results in a cancelled symptom. In most definitions you configure the sensitivity at the symptom level and configure the cancel cycle of alert definition to 1. This configuration ensures that the alert is immediately cancelled after all of the symptoms conditions disappear after the desired symptom cancel cycle.

### Create Alert Definitions to Generate the Fewest Alerts

You can control the size of your alert list and make it easier to manage. When an alert is about a general problem that can be triggered on a large number of objects, configure its definition so that the alert is generated on a higher level object in the hierarchy rather than on individual objects.

As you add symptoms to your alert definition, do not overcrowd a single alert definition with secondary symptoms. Keep the combination of symptoms as simple and straightforward as possible.

You can also use a series of symptom definitions to describe incremental levels of concern. For example, `Volume nearing capacity limit` might have a severity value of `Warning` while `Volume reached capacity limit` might have a severity level of `Critical`. The first symptom is not an immediate threat, but the second one is an immediate threat. You can then include the `Warning` and `Critical` symptom definitions in a single alert definition with an `Any` condition and set the alert criticality to be `Symptom Based`. These settings cause the alert to be generated with the right criticality if either of the symptoms is triggered.

## Avoid Overlapping and Gaps Between Alerts

Overlaps result in two or more alerts being generated for the same underlying condition. Gaps occur when an unresolved alert with lower severity is canceled, but a related alert with a higher severity cannot be triggered.

A gap occurs in a situation where the value is  $\leq 50\%$  in one alert definition and  $\geq 75\%$  in a second alert definition. The gap occurs because when the percentage of volumes with high use falls between 50 percent and 75 percent, the first problem cancels but the second does not generate an alert. This situation is problematic because no alert definitions are active to cover the gap.

## Actionable Recommendations

If you provide text instructions to your users that help them resolve a problem identified by an alert definition, precisely describe how the engineer or administrator should fix the problem to resolve the alert.

To support the instructions, add a link to a wiki, runbook, or other sources of information, and add actions that you run from vRealize Operations Manager on the target systems.

## Creating and Managing vRealize Operations Manager Alert Notifications

When alerts are generated in vRealize Operations Manager, they appear in the alert details and object details, but you can also configure vRealize Operations Manager to send your alerts to outside applications using one or more outbound alert options.

You configure notification options to specify which alerts are sent out for the `Standard Email`, `REST`, `SNMP`, and `Log File` outbound alert plug-ins. For the other plug-in types, all the alerts are sent when the target outbound alert plug-in is enabled.

The most common outbound alert plug-in is the `Standard Email` plug-in. You configure the `Standard Email` plug-in to send notifications to one or more users when an alert is generated that meets the criteria you specify in the notification settings.

## List of Outbound Plug-Ins in vRealize Operations Manager

vRealize Operations Manager provides outbound plug-ins. This list includes the name of the plug-in and whether you can filter the outbound data based on your notification settings.

If the plug-in supports configuring notification rules, then you can filter the messages before they are sent to the target system. If the plug-in does not support notifications, all messages are sent to the target system, and you can process them in that application.

If you installed other solutions that include other plug-in options, they appear as a plug-in option with the other plug-ins.

Messages and alerts are sent only when the plug-in is enabled.

**Table 2-2. Notification Support for Outbound Plug-Ins**

Outbound Plug-In	Configure Notification Rules
Automated Action Plug-in	No The Automated Action plug-in is enabled by default. If automated actions stop working, check the Automated Action plug-in and enable it if necessary. If you edit the Automated Action plug-in, you only need to provide the instance name.
Log File Plug-In	Yes To filter the log file alerts, you can either configure the file named <code>TextFilter.xml</code> or configure the notification rules.
Smarts SAM Notification Plug-In	No
REST Notification Plug-In	Yes
Network Share Plug-In	No
Standard Email Plug-In	Yes
SNMP Trap Plug-In	Yes

## Add Outbound Notification Plug-Ins in vRealize Operations Manager

You add outbound plug-in instances so that you can notify users about alerts or capture alert data outside of vRealize Operations Manager.

You can configure one or more instances of the same plug-in type if you need to direct alert information to multiple target systems.

The Automated Action plug-in is enabled by default. If automated actions stop working, check the Automated Action plug-in and enable it if necessary. If you edit the Automated Action plug-in, you only need to provide the instance name.

- [Add a Standard Email Plug-In for vRealize Operations Manager Outbound Alerts](#)

You add a Standard Email Plug-In so that you can use Simple Mail Transfer Protocol (SMTP) to email vRealize Operations Manager alert notifications to your virtual infrastructure administrators, network operations engineers, and other interested individuals.

- [Add a REST Plug-In for vRealize Operations Manager Outbound Alerts](#)

You add a REST Plug-In so that you can send vRealize Operations Manager alerts to another REST-enabled application where you built a REST Web service to accept these messages.

- [Add a Log File Plug-In for vRealize Operations Manager Outbound Alerts](#)

You add a Log File plug-in when you want to configure vRealize Operations Manager to log alerts to a file on each of your vRealize Operations Manager nodes. If you installed vRealize Operations Manager as a multiple node cluster, each node processes and logs the alerts for the objects that it monitors. Each node logs the alerts for the objects it processes.

- [Add a Network Share Plug-In for vRealize Operations Manager Reports](#)

You add a Network Share plug-in when you want to configure vRealize Operations Manager to send reports to a shared location.

- [Add an SNMP Trap Plug-In for vRealize Operations Manager Outbound Alerts](#)

You add an SNMP Trap plug-in when you want to configure vRealize Operations Manager to log alerts on an existing SNMP Trap server in your environment.

- [Add a Smarts Service Assurance Manager Notification Plug-In for vRealize Operations Manager Outbound Alerts](#)

You add a Smarts SAM Notification plug-in when you want to configure vRealize Operations Manager to send alert notifications to EMC Smarts Server Assurance Manager.

### **Add a Standard Email Plug-In for vRealize Operations Manager Outbound Alerts**

You add a Standard Email Plug-In so that you can use Simple Mail Transfer Protocol (SMTP) to email vRealize Operations Manager alert notifications to your virtual infrastructure administrators, network operations engineers, and other interested individuals.

#### **Prerequisites**

Ensure that you have an email user account that you can use as the connection account for the alert notifications. If you choose to require authentication, you must also know the password for this account.

#### **Procedure**

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon.
- 2 Click **Outbound Settings** and click the plus sign to add a plug-in.
- 3 From the **Plug-In Type** drop-down menu, select **Standard Email Plugin**.

The dialog box expands to include your SMTP settings.

- 4 Enter an **Instance Name**.

This is the name that identifies this instance that you select when you later configure notification rules.

## 5 Configure the SMTP options appropriate for your environment.

Option	Description
<b>Use Secure Connection</b>	Enables secure communication encryption using SSL/TLS. If you select this option, you must select a method in the <b>Secure Connection Type</b> drop-down menu.
<b>Requires Authentication</b>	Enables authentication on the email user account that you use to configure this SMTP instance. If you select this option, you must provide a password for the user account.
<b>SMTP Host</b>	URL or IP address of your email host server.
<b>SMTP Port</b>	Default port SMTP uses to connect with the server.
<b>Secure Connection Type</b>	Select either SSL/TLS as the communication encryption method used in your environment from the drop-down menu. You must select a connection type if you select Use Secure Connection.
<b>User Name</b>	Email user account that is used to connect to the email server.
<b>Password</b>	Password for the connection user account. A password is required if you select Requires Authentication.
<b>Sender Email Address</b>	Email address that appears on the notification message
<b>Sender Name</b>	Displayed name for the sender email address.

## 6 Click **Save**.

## 7 To start the outbound alert service for this plug-in, select the instance in the list and click **Enable** on the toolbar.

This instance of the standard email plug-in for outbound SMTP alerts is configured and running.

### What to do next

Create notification rules that use the standard email plug-in to send a message to your users about alerts requiring their attention. See [User Scenario: Create a vRealize Operations Manager Email Alert Notification](#) .

### Add a REST Plug-In for vRealize Operations Manager Outbound Alerts

You add a REST Plug-In so that you can send vRealize Operations Manager alerts to another REST-enabled application where you built a REST Web service to accept these messages.

The REST Plug-In supports enabling an integration, it does not provide an integration. Depending on your target application, you might need an intermediary REST service or some other mechanism that will correlate the alert and object identifiers included in the REST alert output with the identifiers in your target application.

Determine which content type you are delivering to your target application. If you select application/json, the body of the POST or PUT calls that are sent have the following format. Sample data is included.

```
{
  "startDate":1369757346267,
  "criticality":"ALERT_CRITICALITY_LEVEL_WARNING",
```

```

    "Risk":4.0,
    "resourceId":"sample-object-uuid",
    "alertId":"sample-alert-uuid",
    "status":"ACTIVE",
    "subType":"ALERT_SUBTYPE_AVAILABILITY_PROBLEM",
    "cancelDate":1369757346267,
    "resourceKind":"sample-object-type",
    "alertName":"Invalid IP Address for connected Leaf Switch",
    "attributeKeyID":5325,
    "Efficiency":1.0,
    "adapterKind":"sample-adapter-type",
    "Health":1.0,
    "type":"ALERT_TYPE_APPLICATION_PROBLEM",
    "resourceName":"sample-object-name",
    "updateDate":1369757346267,
    "info":"sample-info"
  }

```

If you select application/xml, the body of the POST or PUT calls that are sent have the following format:

```

<alert>
  <startDate>1369757346267</startDate>
  <criticality>ALERT_CRITICALITY_LEVEL_WARNING</criticality>
  <Risk>4.0</Risk>
  <resourceId>sample-object-uuid</resourceId>
  <alertId>sample-alert-uuid</alertId>
  <status>ACTIVE</status>
  <subType>ALERT_SUBTYPE_AVAILABILITY_PROBLEM</subType>
  <cancelDate>1369757346267</cancelDate>
  <resourceKind>sample-object-type</resourceKind>
  <alertName>Invalid IP Address for connected Leaf Switch</alertName>
  <attributeKeyId>5325</attributeKeyId>
  <Efficiency>1.0</Efficiency>
  <adapterKind>sample-adapter-type</adapterKind>
  <Health>1.0</Health>
  <type>ALERT_TYPE_APPLICATION_PROBLEM</type>
  <resourceName>sample-object-name</resourceName>
  <updateDate>1369757346267</updateDate>
  <info>sample-info</info>
</alert>

```

**Note** If the alert is triggered by a non-metric violation, the `attributeKeyID` is omitted from the REST output and is not sent.

If the request is processed as POST, for either JSON or XML, the Web service returns an HTTP status code of 201, which indicates the alert was successfully created at the target. If the request is processed as PUT, the HTTP status code of 202, which indicates the alert was successfully accepted at the target.

### Prerequisites

Ensure that you know how and where the alerts sent using the REST plug-in are consumed and processed in your environment, and that you have the appropriate connection information available.

## Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon.
- 2 Click **Outbound Settings** and click the plus sign to add a plug-in.
- 3 From the **Plug-In Type** drop-down menu, select **Rest Notification Plugin**.

The dialog box expands to include your REST settings.

- 4 Enter an **Instance Name**.

This is the name that identifies this instance that you select when you later configure notification rules.

- 5 Configure the Rest options appropriate for your environment.

Option	Description
<b>URL</b>	URL to which you are sending the alerts. The URL must support HTTPS. When an alert is sent to the REST Web server, the plug-in appends <code>/{alertID}</code> to the POST or PUT call.
<b>User Name</b>	User account on the target REST system.
<b>Password</b>	User account password.
<b>Content Type</b>	Specify the format for the alert output. <ul style="list-style-type: none"> <li>■ application/json. Alert data is transmitted using JavaScript Object Notation as human-readable text.</li> <li>■ application/xml. Alert data is transmitted using XML that is human-readable and machine-readable content.</li> </ul>
<b>Certificate thumbprint</b>	Thumbprint for the public certificate for your HTTPS service.
<b>Connection count</b>	Limits the number of simultaneous alerts that are sent to the target REST server. Use this number to ensure that your REST server is not overwhelmed with requests.

- 6 Click **Save**.
- 7 To start the outbound alert service for this plug-in, select the instance in the list and click **Enable** on the toolbar.

This instance of the REST plug-in for outbound alerts is configured and running.

## What to do next

Create notification rules that use the REST plug-in to send alerts to a REST-enabled application or service in your environment. See [User Scenario: Create a vRealize Operations Manager REST Alert Notification](#).

## Add a Log File Plug-In for vRealize Operations Manager Outbound Alerts

You add a Log File plug-in when you want to configure vRealize Operations Manager to log alerts to a file on each of your vRealize Operations Manager nodes. If you installed vRealize Operations Manager as a multiple node cluster, each node processes and logs the alerts for the objects that it monitors. Each node logs the alerts for the objects it processes.

All alerts are added to the log file. You can use other applications to filter and manage the logs.

### Prerequisites

Ensure that you have write access to the file system path on the target vRealize Operations Manager nodes.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon.
- 2 Click **Outbound Settings** and click the plus sign to add a plug-in.
- 3 From the **Plug-In Type** drop-down menu, select **Log File**.  
The dialog box expands to include your log file settings.
- 4 In the **Alert Output Folder** text box, enter the folder name.  
If the folder does not exist in the target location, the plug-in creates the folder in the target location.  
The default target location is: `/usr/lib/vmware-vcops/common/bin/`.
- 5 Click **Save**.
- 6 To start the outbound alert service for this plug-in, select the instance in the list and click **Enable** on the toolbar.

This instance of the log file plug-in is configured and running.

### What to do next

When the plug-in is started, the alerts are logged in the file. Verify that the log files are created in the target directory as the alerts are generated, updated, or canceled.

## Add a Network Share Plug-In for vRealize Operations Manager Reports

You add a Network Share plug-in when you want to configure vRealize Operations Manager to send reports to a shared location.

### Prerequisites

Verify that you have read, write, and delete permissions to the network share location.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon.
- 2 Click **Outbound Settings** and click the plus sign to add a plug-in.
- 3 From the **Plug-In Type** drop-down menu, select **Network Share Plug-in**.  
The dialog box expands to include your plug-in instance settings.
- 4 Enter an **Instance Name**.  
This is the name that identifies this instance that you select when you later configure notification rules.

## 5 Configure the Network Share options appropriate for your environment.

Option	Description
<b>Domain</b>	Your shared network domain address.
<b>User Name</b>	The domain user account that is used to connect to the network.
<b>Password</b>	The password for the domain user account.
<b>Network share root</b>	<p>The path to the root folder where you want to save the reports. You can specify subfolders for each report when you configure the schedule publication.</p> <p>You must enter an IP address. For example, <code>\\IP_address\ShareRoot</code>. You can use the host name instead of the IP address if the host name is resolved to an IPv4 when accessed from the vRealize Operations Manager host.</p> <p><b>Note</b> Verify that the root destination folder exists. If the folder is missing, the Network Share plug-in logs an error after 5 unsuccessful attempts.</p>

## 6 Click **Test** to verify the specified paths, credentials, and permissions.

The test might take up to a minute.

## 7 Click **Save**.

The outbound service for this plug-in starts automatically.

## 8 (Optional) To stop an outbound service, select an instance and click **Disable** on the toolbar.

This instance of the Network Share plug-in is configured and running.

### What to do next

Create a report schedule and configure it to send reports to your shared folder.

### Add an SNMP Trap Plug-In for vRealize Operations Manager Outbound Alerts

You add an SNMP Trap plug-in when you want to configure vRealize Operations Manager to log alerts on an existing SNMP Trap server in your environment.

All filtering of the alerts that are sent as SNMP traps must occur on the destination host.

#### Prerequisites

Ensure that you have an SNMP Trap server configured in your environment, and that you know the IP address or host name, port number, and community that it uses.

#### Procedure

1 In the left pane of vRealize Operations Manager, click the **Administration** icon.

2 Click **Outbound Settings** and click the plus sign to add a plug-in.

3 From the **Plug-In Type** drop-down menu, select **SNMP Trap**.

The dialog box expands to include your SNMP trap settings.

4 Type an **Instance Name**.

## 5 Configure the SNMP trap settings appropriate to your environment.

Option	Description
<b>Destination Host</b>	IP address or fully qualified domain name of the SNMP management system to which you are sending alerts.
<b>Port</b>	Port used to connect to the SNMP management system. Default port is 162.
<b>Community</b>	Text string that allows access to the statistics. SNMP Community strings are used only by devices that support SNMPv1 and SNMPv2c protocol.

## 6 Click **Save**.

This instance of the SNMP Trap plug-in is configured and running.

### What to do next

When the plug-in is added, [Configuring Notifications](#) for receiving the SNMP traps.

## Add a Smarts Service Assurance Manager Notification Plug-In for vRealize Operations Manager Outbound Alerts

You add a Smarts SAM Notification plug-in when you want to configure vRealize Operations Manager to send alert notifications to EMC Smarts Server Assurance Manager.

This outbound alert option is useful when you manage the same objects in Server Assurance Manager and in vRealize Operations Manager, and you added the EMC Smarts management pack and configured the solution in vRealize Operations Manager. Although you cannot filter the alerts sent to Service Assurance Manager in vRealize Operations Manager, you can configure the Smarts plug-in to send the alerts to the Smarts Open Integration server. You then configure the Open Integration server to filter the alerts from vRealize Operations Manager, and send only those that pass the filter test to the Smarts Service Assurance Manager service.

### Prerequisites

- Verify that you configured the EMC Smarts solution. For documentation regarding EMC Smarts integration, see <https://solutionexchange.vmware.com/store>.
- Ensure that you have the EMC Smarts Broker and Server Assurance Manager instance host name or IP address, user name, and password.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon.
- 2 Click **Outbound Settings** and click the plus sign to add a plug-in.
- 3 From the **Plug-In Type** drop-down menu, select **Smarts SAM Notification**.

The dialog box expands to include your Smarts settings.

- 4 Enter an **Instance Name**.

This is the name that identifies this instance that you select when you later configure notification rules.

## 5 Configure the Smarts SAM notification settings appropriate for your environment.

Option	Description
<b>Broker</b>	Type the host name or IP address of the EMC Smarts Broker that manages registry for the Server Assurance Manager instance to which you want the notifications sent.
<b>Broker Username</b>	If the Smarts broker is configured as Secure Broker, type the user name for the Broker account.
<b>Broker Password</b>	If the Smarts broker is configured as Secure Broker, type the password for the Broker user account.
<b>SAM Server</b>	Type the host name or IP address of the Server Assurance Manager server to which you are sending the notifications.
<b>User Name</b>	Type the user name for the Server Assurance Manager server instance. This account must have read and write permissions for the notifications on the Smarts server as specified in the SAM Server.
<b>Password</b>	Type the password for the Server Assurance Manager server account.

## 6 Click **Save**.

## 7 Modify the Smarts SAM plug-in properties file.

- a Open the properties file at: `/usr/lib/vmware-vcops/user/plugins/outbound/vcops-smartsalert-plugin/conf/plugin.properties`
- b Add the following string to the properties file: #  
`sendByType=APPLICATION::AVAILABILITY,APPLICATION::PERFORMANCE,APPLICATION::CAPACITY,APPLICATION::COMPLIANCE,VIRTUALIZATION::AVAILABILITY,VIRTUALIZATION::PERFORMANCE,VIRTUALIZATION::CAPACITY,VIRTUALIZATION::COMPLIANCE,HARDWARE::AVAILABILITY,HARDWARE::PERFORMANCE,HARDWARE::CAPACITY,HARDWARE::COMPLIANCE,STORAGE::AVAILABILITY,STORAGE::PERFORMANCE,STORAGE::CAPACITY,STORAGE::COMPLIANCE,NETWORK::AVAILABILITY,NETWORK::PERFORMANCE,NETWORK::CAPACITY,NETWORK::COMPLIANCE`
- c Save the properties file.

## 8 To start the outbound alert service for this plug-in, select the instance in the list and click **Enable** on the toolbar.

This instance of the Smarts SAM Notifications plug-in is configured and running.

### What to do next

In Smarts Service Assurance Manager, configure your Notification Log Console to filter the alerts from vRealize Operations Manager. To configure the filtering for Service Assurance Manager, see the EMC Smarts Service Assurance Manager documentation.

## Filtering Log File Outbound Messages With the TextFilter.xml File

The log file outbound plug-in in vRealize Operations Manager captures alert data. To filter the log file data, you can update the `TextFilter.xml` file to capture only the alerts meeting the filter criteria.

As a vRealize Operations Manager administrator, you want to filter the outbound alert log files based on the alert type and the subtype.

The filters are configured in the `TextFile.xml` file. The file is in the following location:

- vApp or Linux. `/usr/lib/vmware-vcops/user/plugins/outbound/vcops-textfile-plugin/conf`

In the file, use the following format for the filter rule.

```
<FilterRule name="AlertType">
  <AlertTypes>
    <AlertType key="AlertType1:AlertSubType1 " />
    <AlertType key="AlertType2:AlertSubType2 " />
  </AlertTypes>
</FilterRule>
```

For example, the rule to filter based on the Application type and Availability subtype uses this format.

```
<FilterRule name="AlertType">
  <AlertTypes>
    <AlertType key="ALERT_TYPE_APPLICATION_PROBLEM:ALERT_SUBTYPE_AVAILABILITY_PROBLEM " />
  </AlertTypes>
</FilterRule>
```

## Configuring Notifications

Notifications are alert notifications that meet the filter criteria in the notification rules before they are sent outside vRealize Operations Manager. You configure notification rules for the supported outbound alerts so that you can filter the alerts that are sent to the selected external system.

You use the notifications list to manage your rules. You then use the notification rules to limit the alerts that are sent to the external system. To use notifications, the supported outbound alert plug-ins must be added and running.

With notification rules, you can limit the data that is sent to the following external systems.

- Standard Email. You can create multiple notification rules for various email recipients based on one or more of the filter selections. If you add recipients but do not add filter selections, all the generated alerts are sent to the recipients.
- REST. You can create a rule to limit alerts that are sent to the target REST system so that you do not need to implement filtering on that target system.
- SNMP Trap. You can configure vRealize Operations Manager to log alerts on an existing SNMP Trap server in your environment.
- Log File. You can configure vRealize Operations Manager to log alerts to a file on each of your vRealize Operations Manager nodes.

### User Scenario: Create a vRealize Operations Manager Email Alert Notification

As a virtual infrastructure administrator, you need vRealize Operations Manager to send email notifications to your advanced network engineers when critical alerts are generated for mmbhost object,

the host for many virtual machines that run transactional applications, where no one has yet taken ownership of the alert.

### Prerequisites

- Ensure that you have at least one alert definition for which you are sending a notification. For an example of an alert definition, see [Create an Alert Definition for Department Objects](#).
- Ensure that at least one instance of the standard email plug-in is configured and running. See [Add a Standard Email Plug-In for vRealize Operations Manager Outbound Alerts](#).

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon.
- 2 Click **Notifications** and click the plus sign to add a notification rule.
- 3 In the **Name** text box type a name similar to **Unclaimed Critical Alerts for mmbhost**.
- 4 In the Method area, select **Standard Email Plug-In** from the drop-down menu, and select the configured instance of the email plug-in.
- 5 Configure the email options.
  - a In the **Recipients** text box, type the email addresses of the members of your advance engineering team, separating the addresses with a semi-colon (;).
  - b To send a second notification if the alert is still active after a specified amount of time, type the number of minutes in the **Notify again** text box.
  - c Type number of notifications that are sent to users in the **Max Notifications** text box.
- 6 Configure the scope of filtering criteria.
  - a From the **Scope** drop-down menu, select **Object**.
  - b Click **Click to select Object** and type the name of the object.  
In this example, type **mmbhost**.
  - c Locate and select the object in the list, and click **Select**.
- 7 Configure the Notification Trigger.
  - a From the **Notification Trigger** drop-down menu, select **Impact**.
  - b From the adjacent drop-down menu, select **Health**.
- 8 In the Criticality area, click **Critical**.
- 9 Expand the Advanced Filters and from the **Alert States** drop-down menu, select **Open**.  
The Open state indicates that no engineer or administrator has taken ownership of the alert.
- 10 Click **Save**.

You created a notification rule that sends an email message to the members of your advance network engineering team when any critical alerts are generated for the mmbhost object and the alert is not claimed by an engineer. This email reminds them to look at the alert, take ownership of it, and work to resolve the triggering symptoms.

### What to do next

Respond to alert email notifications. See *vRealize Operations Manager User Guide*.

### User Scenario: Create a vRealize Operations Manager REST Alert Notification

As a virtual infrastructure administrator, you need vRealize Operations Manager to send alerts in JSON or XML to a REST-enabled application that has REST Web service that accepts these messages. You want only alerts where the virtualization alerts that affect availability alert types go to this outside application. You can then use the provided information to initiate a remediation process in that application to address the problem indicated by the alert.

The notification configuration limits the alerts sent to the outbound alert instance to those matching the notification criteria.

### Prerequisites

- Verify that you have at least one alert definition for which you are sending a notification. For an example of an alert definition, see [Create an Alert Definition for Department Objects](#).
- Verify that at least one instance of the REST plug-in is configured and running. See [Add a REST Plug-In for vRealize Operations Manager Outbound Alerts](#).

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon.
- 2 Click **Notifications** and click the plus sign to add a notification rule.
- 3 In the **Name** text box type a name similar to **Virtualization Alerts for Availability**.
- 4 In the Method area, select **REST Plug-In** from the drop-down menu, and select the configured instance of the email plug-in.
- 5 Configure the Notification Trigger.
  - a From the **Notification Trigger** drop-down menu, select **Alert Type**.
  - b Click **Click to select Alert type/subtype** and select **Virtualization/Hypervisor Alerts Availability**.
- 6 In the Criticality area, click **Warning**.
- 7 Expand the Advanced Filters and from the **Alert Status** drop-down menu, select **New**.  
The New status indicates that the alert is new to the system and not updated.
- 8 Click **Save**.

You created a notification rule that sends the alert text to the target REST-enabled system. Only the alerts where the configured alert impact is Virtualization/Hypervisor Availability and where the alert is configured as a warning are sent to the target instance using the REST plug-in.

## Create an Alert Definition for Department Objects

As a virtual infrastructure administrator, you are responsible for the virtual machines and hosts that the accounting department uses. You can create alerts to manage the accounting department objects.

You received several complaints from your users about delays when they are using their accounting applications. Using vRealize Operations Manager, you identified the problem as related to CPU allocations and workloads. To better manage the problem, you create an alert definition with tighter symptom parameters so that you can track the alerts and identify problems before your users encounter further problems.

Using this scenario, you create a monitoring system that monitors your accounting objects and provides timely notifications when problems occur.

### Add Description and Base Object to Alert Definition

To create an alert to monitor the CPUs for the accounting department virtual machines and monitor host memory for the hosts on which they operate, you begin by describing the alert.

When you name the alert definition and define alert impact information, you specify how the information about the alert appears in vRealize Operations Manager. The base object is the object around which the alert definition is created. The symptoms can be for the base object and for related objects.

#### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon.
- 2 Click **Alert Definitions**.
- 3 Click the plus sign to add a definition.
- 4 Type a name and description.

In this scenario, type **Acct VM CPU early warning** as the alert name, which is a quick overview of the problem. The description, which is a detailed overview, should provide information that is as useful as possible. When the alert is generated, this name and description appears in the alert list and in the notification.

- 5 Click **Base Object Type**.
- 6 From the drop-down menu, expand **vCenter Adapter** and select **Host System**.

This alert is based on host systems because you want an alert that acts as an early warning to possible CPU stress on the virtual machines used in the accounting department. By using host systems as the based object type, you can respond to the alert symptom for the virtual machines with bulk actions rather than responding to an alert for each virtual machine.

7 Click **Alert Impact** and configure the metadata for this alert definition.

- a From the **Impact** drop-down menu, select **Risk**.

This alert indicates a potential problem and requires attention in the near future.

- b From the **Criticality** drop-down menu, select **Immediate**.

As a Risk alert, which is indicative of a future problem, you still want to give it a high criticality so that it is ranked for correct processing. Because it is designed as an early warning, this configuration provides a built-in buffer that makes it an immediate risk rather than a critical risk.

- c From the **Alert Type and Subtype** drop-down menu, expand **Virtualization/Hypervisor** and select **Performance**.

- d To ensure that the alert is generated during the first collection cycle after the symptoms become true, set the **Wait Cycle** to **1**.

- e To ensure that the an alert is removed as soon as the symptoms are no longer triggered, set the **Cancel Cycle** to **1**.

The alert is canceled in the next collection cycle if the symptoms are no long true.

These alert impact options help you identify and prioritize alerts as they are generated.

You started an alert definition where you provided the name and description, selected host system as the base object type, and defined the data that appears when the alert generated.

#### What to do next

Continue in the workspace, adding symptoms to your alert definition. See [Add a Virtual Machine CPU Usage Symptom to the Alert Definition](#).

## Add a Virtual Machine CPU Usage Symptom to the Alert Definition

To generate alerts related to CPU usage on your accounting virtual machines, you add symptoms to your vRealize Operations Manager alert definition after you provide the basic descriptive information for the alert. The first symptom you add is related to CPU usage on virtual machines. You later use a policy and group to apply alert to the accounting virtual machines.

This scenario has two symptoms, one for the accounting virtual machines and one to monitor the hosts on which the virtual machines operate.

#### Prerequisites

Begin configuring the alert definition. See [Add Description and Base Object to Alert Definition](#).

#### Procedure

- 1 In the **Alert Definition Workspace** window, after you configure the **Name and Description**, **Base Object Type**, and **Alert Impact**, click **Add Symptom Definitions** and configure the symptoms.

- 2 Begin configuring the symptom set related to virtual machines CPU usage.
  - a From the **Defined On** drop-down menu, select **Child**.
  - b From the **Filter by Object Type** drop-down menu, select **Virtual Machine**.
  - c From the **Symptom Definition Type** drop-down menu, select **Metric / Supermetric**.
  - d Click the **Add** button to open the **Add Symptom Definition** workspace window.

- 3 Configure the virtual machine CPU usage symptom in the **Add Symptom Definition** workspace window.

- a From the **Base Object Type** drop-down menu, expand **vCenter Adapter** and select **Virtual Machine**.

The collected metrics for virtual machines appears in the list.

- b In the metrics list **Search** text box, which searches the metric names, type **usage**.

- c In the list, expand **CPU** and drag **Usage (%)** to the workspace on the right.

- d From the threshold drop-down menu, select **Dynamic Threshold**.

Dynamic thresholds use vRealize Operations Manager analytics to identify the trend metric values for objects.

- e In the **Symptom Definition Name** text box, type a name similar to **VM CPU Usage above trend**.

- f From the criticality drop-down menu, select **Warning**.

- g From the threshold drop-down menu, select **Above Threshold**.

- h Leave the **Wait Cycle** and **Cancel Cycle** at the default values of 3.

This Wait Cycle setting requires the symptom condition to be true for 3 collection cycles before the symptom is triggered. This wait avoids triggering the symptom when there is a short spike in CPU usage.

- i Click **Save**.

The dynamic symptom, which identifies when the usage is above the tracked trend, is added to the symptom list.

- 4 In the **Alert Definition Workspace** window, drag **VM CPU Usage above trend** from the symptom definition list to the symptom workspace on the right.

The Child-Virtual Machine symptom set is added to the symptom workspace.

- 5 In the symptoms set, configure the triggering condition so that when the symptom is true on half of the virtual machines in the group to which this alert definition is applied, the symptom set is true.

- a From the value operator drop-down menu, select **>**.

- b In the value text box, enter **50**.

- c From the value type drop-down menu, select **Percent**.

You defined the first symptom set for the alert definition.

### What to do next

Add the host memory usage symptom to the alert definition. See [Add a Host Memory Usage Symptom to the Alert Definition](#).

## Add a Host Memory Usage Symptom to the Alert Definition

To generate alerts related to CPU usage on your accounting virtual machines, you add a second symptom to your vRealize Operations Manager alert definition after you add the first symptom. The second symptom is related to host memory usage for the hosts on which the accounting virtual machines operate.

### Prerequisites

Add the virtual machine CPU usage symptom. See [Add a Virtual Machine CPU Usage Symptom to the Alert Definition](#).

### Procedure

- 1 In the **Alert Definition Workspace** window, after you configure the **Name and Description**, **Base Object Type**, and **Alert Impact**, click **Add Symptom Definitions**.
- 2 Configure the symptom related to host systems for the virtual machines.
  - a From the **Defined On** drop-down menu, select **Self**.
  - b From the **Symptom Definition Type** drop-down menu, select **Metric / Supermetric**.
  - c Click the **Add** button to configure the new symptom.
- 3 Configure the host system symptom in the **Add Symptom Definition** workspace window.
  - a From the **Base Object Type** drop-down menu, expand **vCenter Adapters** and select **Host System**.
  - b In the metrics list, expand **Memory** and drag **Usage (%)** to the workspace on the right.
  - c From the threshold drop-down menu, select **Dynamic Threshold**.

Dynamic thresholds use vRealize Operations Manager analytics to identify the trend metric values for objects.
  - d In the **Symptom Definition Name** text box, enter a name similar to **Host memory usage above trend**.
  - e From the criticality drop-down menu, select **Warning**.
  - f From the threshold drop-down menu, select **Above Threshold**.

- g Leave the **Wait Cycle** and **Cancel Cycle** at the default values of 3.

This Wait Cycle setting requires the symptom condition to be true for three collection cycles before the symptom is triggered. This wait avoids triggering the symptom when a short spike occurs in host memory usage.

- h Click **Save**.

The dynamic symptom identifies when the hosts on which the accounting virtual machines run are operating above the tracked trend for memory usage.

The dynamic symptom is added to the symptom list.

- 4 In the **Alert Definition Workspace** window, drag **Host memory usage above trend** from the symptoms list to the symptom workspace on the right.

The Self-Host System symptom set is added to the symptom workspace.

- 5 On the Self-Host System symptom set, from the value type drop-down menu for **This Symptom set is true when**, select **Any**.

With this configuration, when any of the hosts running accounting virtual machines exhibit memory usage that is above the analyzed trend, the symptom condition is true.

- 6 At the top of the symptom set list, from the **Match {operator} of the following symptoms** drop-down menu, select **Any**.

With this configuration, if either of the two symptom sets, virtual machine CPU usage or the host memory, are triggered, an alert is generated for the host.

You defined the second symptom set for the alert definition and configured how the two symptom sets are evaluated to determine when the alert is generated.

### What to do next

Add recommendations to your alert definition so that you and your engineers know how to resolve the alert when it is generated. See [Add Recommendations to the Alert Definition](#).

## Add Recommendations to the Alert Definition

To resolve a generated alert for the accounting department's virtual machines, you provide recommendations so that you or other engineers have the information you need to resolve the alert before your users encounter performance problems.

As part of the alert definition, you add recommendations that include actions that you run from vRealize Operations Manager and instructions for making changes in vCenter Server that resolve the generated alert.

### Prerequisites

Add symptoms to your alert definition. See [Add a Host Memory Usage Symptom to the Alert Definition](#).

## Procedure

- 1 In the **Alert Definition Workspace** window, after you configure the **Name and Description**, **Base Object Type**, **Alert Impact**, and **Add Symptom Definitions**, click **Add Recommendations** and add the recommended actions and instructions.
- 2 Click **Add** and select an action recommendation to resolve the virtual machine alerts.
  - a In the **New Recommendation** text box, enter a description of the action similar to **Add CPUs to virtual machines**.
  - b From the **Actions** drop-down menu, select **Set CPU Count for VM**.
  - c Click **Save**.
- 3 Click **Add** and provide an instructive recommendation to resolve host memory problems similar to this example.
 

**If this host is part of a DRS cluster, check the DRS settings to verify that the load balancing setting are configured correctly. If necessary, manually vMotion the virtual machines.**
- 4 Click **Add** and provide an instructive recommendation to resolve host memory alerts.
  - a Enter a description of the recommendation similar to this example.
 

**If this is a standalone host, add more memory to the host.**
  - b To make the URL a hyperlink in the instructions, copy the URL, for example, <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>, to your clipboard.
  - c Highlight the text in the text box and click **Create a hyperlink**.
  - d Paste the URL in the **Create a hyperlink** text box and click **OK**.
  - e Click **Save**.
- 5 In the **Alert Definition Workspace**, drag **Add CPUs to virtual machines**, **If this host is part of a DRS cluster**, and the **If this is a standalone host** recommendations from the list to the recommendation workspace in the order presented.
- 6 Click **Save**.

You provided the recommended actions and instructions to resolve the alert when it is generated. One of the recommendations resolves the virtual machine CPU usage problem and the other resolves the host memory problem.

## What to do next

Create a group of objects to use to manage your accounting objects. See [Create a Custom Accounting Department Group](#).

## Create a Custom Accounting Department Group

To manage, monitor, and apply policies to the accounting objects as a group, you create a custom object group.

## Prerequisites

Verify that you completed the alert definition for this scenario. See [Add Recommendations to the Alert Definition](#).

## Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Environment** icon.
- 2 Click the **Groups** tab.
- 3 Click **New Group**.
- 4 Type a name similar to **Accounting VMs and Hosts**.
- 5 From the **Group Type** drop-down menu, select **Department**.
- 6 From the **Policy** drop-down menu, select **Default Policy**.

When you create a policy, you apply the new policy to the accounting group.

- 7 In the Define membership criteria area, from the **Select the Object Type that matches the following criteria** drop-down menu, expand **vCenter Adapter**, select **Host System**, and configure the dynamic group criteria.
  - a From the criteria drop-down menu, select **Relationship**.
  - b From the relationships options drop-down menu, select **Parent of**.
  - c From the operator drop-down menu, select **contains**.
  - d In the **Object name** text box, enter **acct**.
  - e From the navigation tree drop-down list, select **vSphere Hosts and Clusters**.

You created a dynamic group where host objects that are the host for virtual machines with acct in the virtual machine name are included in the group. If a virtual machine with acct in the object name is added or moved to a host, the host object is added to the group.

- 8 Click **Preview** in the lower-left corner of the workspace, and verify that the hosts on which your virtual machines that include acct in the object name appear in the **Preview Group** window.
- 9 Click **Close**.
- 10 Click **Add another criteria set**.

A new criteria set is added with the OR operator between the two criteria sets.

- 11 From the **Select the Object Type that matches the following criteria** drop-down menu, expand **vCenter Adapter**, select **Virtual Machine**, and configure the dynamic group criteria.
  - a From the criteria drop-down menu, select **Properties**.
  - b From the **Pick a property** drop-down menu, expand **Configuration** and double-click **Name**.
  - c From the operator drop-down menu, select **contains**.
  - d In the **Property value** text box, enter **acct**.

You created a dynamic group where virtual machine objects with acct in the object name are included in the group that depends on the presence of those virtual machines. If a virtual machine with acct in the name is added to your environment, it is added to the group.

**12** Click **Preview** in the lower-left corner of the workspace, and verify that the virtual machines with acct in the object name are added to the list that also includes the host systems.

**13** Click **Close**.

**14** Click **OK**.

The Accounting VMs and Hosts group is added to the Groups list.

You created a dynamic object group that changes as virtual machines with acct in their names are added, removed, and moved in your environment.

### What to do next

Create a policy that determines how vRealize Operations Manager uses the alert definition to monitor your environment. See [Create a Policy for the Accounting Alert](#).

## Create a Policy for the Accounting Alert

To configure how vRealize Operations Manager evaluates the accounting alert definition in your environment, you configure a policy that determines behavior so that you can apply the policy to an object group. The policy limits the application of the alert definition to only the members of the selected object group.

When an alert definition is created, it is added to the default policy and enabled, ensuring that any alert definitions that you create are active in your environment. This alert definition is intended to meet the needs of the accounting department, so you disable it in the default policy and create a new policy to govern how the alert definition is evaluated in your environment, including which accounting virtual machines and related hosts to monitor.

### Prerequisites

- Verify that you completed the alert definition for this scenario. See [Add Recommendations to the Alert Definition](#).
- Verify that you created a group of objects that you use to manage your accounting objects. See [Create a Custom Accounting Department Group](#).

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon.
- 2 Click **Policies** and click **Policy Library**.
- 3 Click **Add New Policy**.

- 4 Type a name similar to **Accounting Objects Alerts Policy** and provide a useful description similar to the following example.

```
This policy is configured to generate alerts when
Accounting VMs and Hosts group objects are above trended
CPU or memory usage.
```

- 5 Click **Select Base Policies** and select **Default Policy** from the **Start with** drop-down menu.
- 6 On the left, click **Customize Alert / Symptom Definitions** and disable all the alert definitions except the new Acct VM CPU early warning alert.
  - a In the Alert Definitions area, click **Actions** and select **Select All**.  
The alerts on the current page are selected.
  - b Click **Actions** and select **Disable**.  
The alerts indicate Disabled in the State column.
  - c Repeat the process on each page of the alerts list.
  - d Select **Acct VM CPU early warning** in the list, click **Actions** and select **Enable**.  
The Acct VM CPU early warning alert is now enabled.
- 7 On the left, click **Apply Policy to Groups** and select **Accounting VMs and Hosts**.
- 8 Click **Save**.

You created a policy where the accounting alert definition exists in a custom policy that is applied only to the virtual machines and hosts for the accounting department.

#### What to do next

Create an email notification so that you learn about alerts even you when you are not actively monitoring vRealize Operations Manager. See [Configure Notifications for the Department Alert](#).

## Configure Notifications for the Department Alert

To receive an email notification when the accounting alert is generated, rather than relying on your ability to generally monitor the accounting department objects in vRealize Operations Manager, you create notification rules.

Creating an email notification when accounting alerts are triggered is an optional process, but it provides you with the alert even when you are not currently working in vRealize Operations Manager.

#### Prerequisites

- Verify that you completed the alert definition for this scenario. See [Add Recommendations to the Alert Definition](#).
- Verify that standard email outbound alerts are configured in your system. See [Add a Standard Email Plug-In for vRealize Operations Manager Outbound Alerts](#).

## Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon.
- 2 Click **Notifications** and click the plus sign to add a notification rule.
- 3 Configure the communication options.
  - a In the **Name** text box, type a name similar to **Acct Dept VMs or Hosts Alerts**.
  - b From the **Select Plug-In Type** drop-down menu, select **StandardEmailPlugin**.
  - c From the **Select Instance** drop-down menu, select the standard email instance that is configured to send messages.
  - d In the **Recipients** text box, type your email address and the addresses of other recipients responsible for the accounting department alerts. Use a semicolon between recipients.
  - e Leave the **Notify again** text box blank.

If you do not provide a value, the email notice is sent only once. This alert is a Risk alert and is intended as an early warning rather than requiring an immediate response.

You configured the name of the notification when it is sent to you and the method that is used to send the message.

- 4 In the Filtering Criteria area, configure the accounting alert notification trigger.
  - a From the **Notification Trigger** drop-down menu, select **Alert Definition**.
  - b Click **Click to select Alert Definition**.
  - c Select **Acct VM CPU early warning** and click **Select**.
- 5 Click **Save**.

You created a notification rule that sends you and your designated engineers an email message when this alert is generated for your accounting department alert definition.

## What to do next

Create a dashboard with alert-related widgets so that you can monitor alerts for the accounting object group. See [Create a Dashboard to Monitor Department Objects](#).

## Create a Dashboard to Monitor Department Objects

To monitor all the alerts related to the accounting department object group, you create a dashboard that includes the alert list and other widgets. The dashboard provides the alert data in a single location for all related objects.

Creating a dashboard to monitor the accounting virtual machines and related hosts is an optional process, but it provides you with a focused view of the accounting object group alerts and objects.

## Prerequisites

Create an object group for the accounting department virtual machines and related objects. See [Create a Custom Accounting Department Group](#).

## Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Dashboards**.
- 2 Click **Add**.
- 3 In the Dashboard Configuration definition area, type a tab name similar to **Accounting VMs and Hosts** and configure the layout options.
- 4 Click **Widget List** and drag the following widgets to the workspace.

- **Alert List**
- **Efficiency**
- **Health**
- **Risk**
- **Top Alerts**
- **Alert Volume**

The blank widgets are added to the workspace. To change the order in which they appear, you can drag them to a different location in the workspace.

- 5 On the Alert List widget title bar, click **Edit Widget** and configure the settings.

- a In the **Title** text box, change the title to **Acct Dept Alert List**.
- b For the **Refresh Content** option, select **On**.
- c Type **Accounting** in the **Search** text box and click **Search**.

The Accounting value corresponds to the name of the object group for the accounting department virtual machines and related hosts.

- d In the filtered resource list, select the **Accounting VMs and Hosts** group.

The Accounting VMs and Hosts group is identified in the Selected Resource text box.

- e Click **OK**.

The Acct Dept Alert List is now configured to display alerts for the Accounting VMs and Hosts group objects.

- 6 Click **Widget Interactions** and configure the following interactions.

- a For Acct Dept Alert List, leave the selected resources blank.
- b For Top Alerts, Health, Risk, Efficiency, and Alert Volume select **Acct Dept Alert List** from the **Selected Resources** drop-down menu.
- c Click **Apply Interactions**.

With the widget interaction configured in this way, the select alert in the Acct Dept Alert List is the source for the data in the other widgets. When you select an alert in the alert list, the Health, Risk, and Efficiency widgets display alerts for that object, Top Alerts displays the topic issues affecting the health of the object, and Alert Volume displays an alert trend chart.

## 7 Click **Save**.

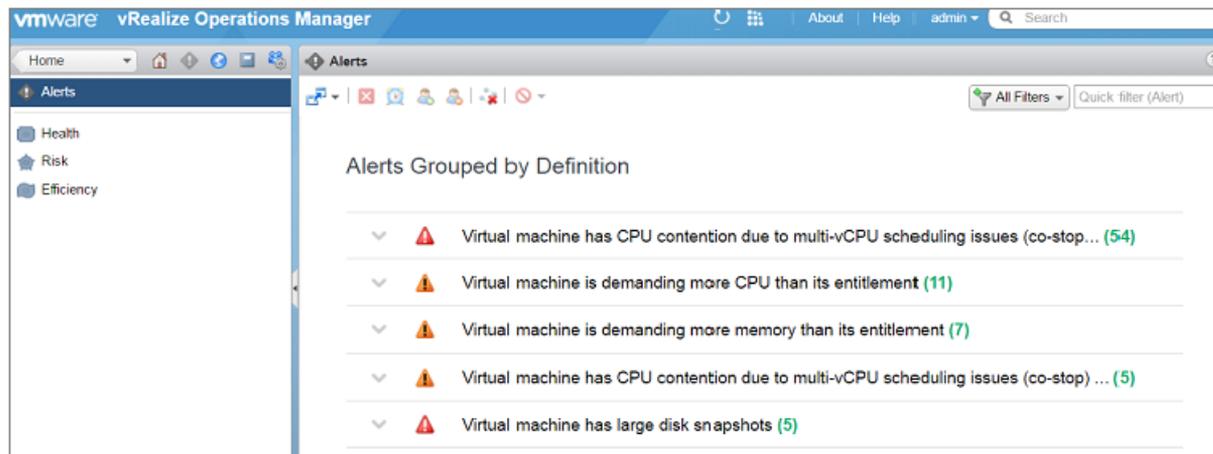
You created a dashboard that displays the alerts related to the accounting virtual machines and hosts group, including the Risk alert you created.

## Alerts Group

For easy and better management of alerts, you can arrange them as a group as per your requirement.

It is complicated to identify a problem in large environments as you receive different kind of alerts. To manage alerts easily, group them by their definitions.

For example, there are 1000 alerts in your system. To identify different types of alerts, group them based on their alert definitions. It is also easy to detect the alert having the highest severity in the group.



When you group alerts, you can see the number of times the alerts having the same alert definition are triggered. By grouping alerts, you can perform the following tasks easily and quickly:

- Find the noisiest alert: The alert that has triggered maximum number of times is known as the noisiest alert. Once you find it, you can disable it to avoid further noise.
- Filter alerts: You can filter alerts based on a substring in alert definitions. The result shows the group of alerts that contain the substring.

### Note

- If you cancel or disable an alert group, the alerts are not canceled instantly. It might take some time if the group is large.
- Only one group can be expanded at a time.
- The number next to the group denotes the number of alerts in that particular group.
- The criticality sign  indicates the highest level of severity of an alert in a group.

## Grouping Alerts

To group alerts:

### Procedure

- 1 Click **Alerts** in the left pane of vRealize Operations Manager.
- 2 Click  to group the alerts

## Ungrouping Alerts

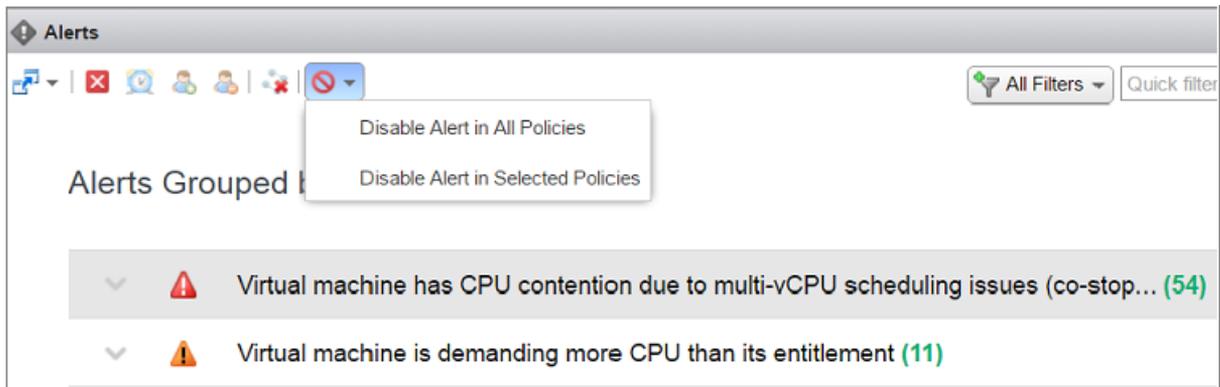
To ungroup alerts:

### Procedure

- 1 Click **Alerts** in the left pane of vRealize Operations Manager.
- 2 Click  to ungroup the alerts

## Disable Alerts

In an alerts group, you can disable an alert by a single click.



The alerts can be disabled by two methods:

- **Disable Alert in All Policies:** You disable the alert for all the objects for all the policies.
- **Disable Alert in Selected Policies:** You disable the alert for the objects having the selected policy. Note that this method will work only for objects with alerts.

## Configuring Actions

Actions are the ability to update objects or read data about objects in monitored systems, and are commonly provided in vRealize Operations Manager as part of a solution. The actions added by solutions are available from the object Actions menu, list and view menus, including some dashboard widgets, and can be added to alert definition recommendations.

The possible actions include read actions and update actions.

The read actions retrieve data from the target objects.

The update actions modifies the target objects. For example, you can configure an alert definition to notify you when a virtual machine is experiencing memory issues. Add an action in the recommendations that runs the Set Memory for Virtual Machine action. This action increases the memory and resolves the likely cause of the alert.

To see or use the actions for your vCenter Server objects, you must enable actions in the vCenter Adapter for each monitored vCenter Server instance. Actions can only be viewed and accessed if you have the required permissions.

## List of vRealize Operations Manager Actions

The list of actions includes the name of the action, the objects that each one modifies, and the object levels at which you can run the action. You use this information to ensure that you correctly apply the actions as alert recommendations and when the actions are available in the **Actions** menu.

### Actions and Modified Objects

vRealize Operations Manager actions make changes to objects in your managed vCenter Server instances.

When you grant a user access to actions in vRealize Operations Manager, that user can take the granted action on any object that vRealize Operations Manager manages, and not only on objects that the user can access outside of vRealize Operations Manager.

### Action Object Levels

The actions are available when you work with different object levels, but they modify only the specified object. If you are working at the cluster level and select **Power On VM**, all the virtual machines in the cluster for which you have access permission are available for you to run the action. If you are working at the virtual machine level, only the selected virtual machine is available.

**Table 2-3. vRealize Operations Manager Actions Affected Objects**

Action	Modified Object	Object Levels
Rebalance Container	Virtual Machines	<ul style="list-style-type: none"> <li>■ Data Center</li> <li>■ Custom Data Center</li> </ul>
Delete Idle VM	Virtual Machines	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Set DRS Automation	Cluster	<ul style="list-style-type: none"> <li>■ Clusters</li> </ul>
Move VM	Virtual Machine	<ul style="list-style-type: none"> <li>■ Virtual Machines</li> </ul>
Power Off VM	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Shut Down Guest OS for VM	Virtual Machine VMware Tools must be installed and running on the target virtual machines to run this action.	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>

Action	Modified Object	Object Levels
Power On VM	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Delete Powered Off VM	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Set Memory for VM and Set Memory for VM Power Off Allowed	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Set Memory Resources for VM	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Set CPU Count for VM and Set CPU Count for VM Power Off Allowed	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Set CPU Resources for VM	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Set CPU Count and Memory for VM and Set CPU Count and Memory for VM Power Off Allowed	Virtual Machine	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Delete Unused Snapshots for VM	Snapshot	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Host Systems</li> <li>■ Virtual Machines</li> </ul>
Delete Unused Snapshots for Datastore	Snapshot	<ul style="list-style-type: none"> <li>■ Clusters</li> <li>■ Datastores</li> <li>■ Host Systems</li> </ul>

## Actions Supported for Automation

Recommendations can identify ways to remediate problems indicated by an alert. Some of these remediations can be associated with actions defined in your vRealize Operations Manager instance. You can automate several of these remediation actions for an alert when that recommendation is the first priority for that alert.

You enable actionable alerts in your policies. By default, automation is disabled in policies. To configure automation for your policy, you select **Administration > Policies > Policy Library**. Then, you edit a policy, access the **Alert / Symptom Definitions** workspace, and select **Local** for the **Automate** setting in the Alert Definitions pane.

When an action is automated, you can use the **Automated** and **Alert** columns in **Administration > Recent Tasks** to identify the automated action and view the results of the action.

- vRealize Operations Manager uses the **automationAdmin** user account to trigger automated actions. For these automated actions that are triggered by alerts, the Submitted By column displays the **automationAdmin** user.
- The Alert column displays the alert that triggered the action. When an alert is triggered that is associated to the recommendation, it triggers the action without any user intervention.

The following actions are supported for automation:

- Delete Powered Off VM
- Delete Idle VM
- Move VM
- Power Off VM
- Power On VM
- Set CPU Count And Memory for VM
- Set CPU Count And Memory for VM Power Off Allowed
- Set CPU Count for VM
- Set CPU Count for VM Power Off Allowed
- Set CPU Resources for VM
- Set Memory for VM
- Set Memory for VM Power Off Allowed
- Set Memory Resources for VM
- Shut Down Guest OS for VM



How to Use Alerts and Actions Together for Automation

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_vrealize\\_alerts\\_actions\\_automation](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrealize_alerts_actions_automation))



How to Automate an Alert that has an Associated Action

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_vrom\\_automate\\_alert\\_with\\_action](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrom_automate_alert_with_action))



How to Create and Automate a New Alert with a Symptom Definition and Action

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_vrom\\_create\\_alert\\_automate\\_symptom\\_definition](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrom_create_alert_automate_symptom_definition))

## Roles Needed to Automate Actions

To automate actions, your role must have the following permissions:

- Create, edit, and import policies in **Administration > Policy Management**.

- Create, clone, edit, and import alert definitions in **Content > Alert Definition Management**.
- Create, edit, and import recommendation definitions in **Content > Recommendations Management**.

---

**Important** You set the permissions used to run the actions separately from the alert and recommendation definition. Anyone who can modify alerts, recommendations, and policies can also automate the action, even if they do not have permission to run the action.

---

For example, if you do not have access to the Power Off VM action, but you can create and modify alerts and recommendations, you can see the Power Off VM action and assign it to an alert recommendation. Then, if you automate the action in your policy, vRealize Operations Manager uses the automationAdmin user to run the action.

### Example Action Supported for Automation

For the Alert Definition named `Virtual machine has chronic high CPU workload leading to CPU stress`, you can automate the action named `Set CPU Count for VM`.

When CPU stress on your virtual machines exceeds a critical, immediate, or warning level, the alert triggers the recommended action without user intervention.

## Integration of Actions with vRealize Automation

vRealize Operations Manager restricts actions on objects that vRealize Automation manages, so that the actions do not violate any constraints set forth by vRealize Automation.

When objects in your environment are managed by vRealize Automation, actions in vRealize Operations Manager are not available on those objects. For example, if a host or parent object is being managed by vRealize Automation, actions are not available on that object.

This behavior is true for all actions, including **Power Off VM**, **Move VM**, **Rebalance Container**, and so on.

You cannot turn on or turn off the exclusion of actions on vRealize Automation managed objects.

### Actions Determine Whether Objects Are Managed

Actions check the objects in the vRealize Automation managed resource container to determine which objects are being managed by vRealize Automation.

- Actions such as **Rebalance Container** check the child objects of the data center container or custom data center container to determine whether the objects are managed by vRealize Automation. If the objects are being managed, the action does not appear on those objects.

- The Move VM action checks whether the virtual machine to be moved is being managed by vRealize Automation.

Is the Virtual Machine Managed?	Result of Move VM Action
Yes	The Move VM action does not appear in the vRealize Operations Manager user interface for that virtual machine.
No	The Move VM action moves the virtual machine to a new host, datastore, or new host and datastore. The Move VM action does not check whether the new host or datastore is being managed by vRealize Automation.

- The Delete Snapshots action checks whether the virtual machine or datastore is being managed by vRealize Automation.

## Actions on Objects that vRealize Automation Does Not Manage

For a host or parent object that is not managed by vRealize Automation, only the virtual machines that are not being managed by vRealize Automation appear in the action dialog, and you can only take action on the virtual machines that are not being managed by vRealize Automation. If all child objects are being managed by vRealize Automation, the user interface displays the message `No objects are eligible` for the selected action.

## If You Attempt to Run an Action on Multiple Objects

If you select multiple objects and attempt to run an action, such as Power Off VM, only the objects that are not being managed by vRealize Automation, which might include a subset of the virtual machines, appear in the Power Off VM action dialog box.

## Working With Actions That Use Power Off Allowed

Some of the actions provided with vRealize Operations Manager require the virtual machines to shut down or power off, depending on the configuration of the target machines, to run the actions. You should understand the impact of the Power Off Allowed option before running the actions so that you select the best options for your target virtual machines.

## Power Off and Shut Down

The actions that you can run on your vCenter Server instances include actions that shut down virtual machines and actions that power off virtual machines. It also includes actions where the virtual machine must be in a powered off state to complete the action. Whether the virtual machine is shut down or powered off depends on how it is configured and what options you select when you run the action.

The shut down action shuts down the guest operating system and then powers off the virtual machine. To shut down a virtual machine from vRealize Operations Manager, the VMware Tools must be installed and running on the target objects.

The power off action turns the virtual machine off without regard for the state of the guest operating system. In this case, if the virtual machine is running applications, your user could lose data. After the action is finished, for example, modifying the CPU count, the virtual machine is returned to the power state it was in when the action began.

## Power Off Allowed and VMware Tools

For the actions where you are increasing the CPU count or the amount of memory on a virtual machine, some operating systems support the actions if the Hot Plug is configured on the virtual machine, but for other operating systems, the virtual machine must be in a powered off state to change the configuration. To accommodate this need where the VMware Tools are not running, the Set CPU Count, Set Memory, and Set CPU Count and Memory actions include the Power Off Allowed option.

If you select Power Off Allowed, and the machine is running, the action verifies whether VMware Tools is installed and running.

- If VMware Tools are installed and running, the virtual machine is shut down before completing the action.
- If VMware Tools are not running or not installed, the virtual machine is powered off without regard for the state of the operating system.

If you do not select Power Off Allowed and you are decreasing the CPU count or memory, or the hot plug is not enabled for increasing the CPU count or memory, the action does not run and the failure is reported in Recent Tasks.

## Power Off Allowed When Changing CPU Count or Memory

When you run the actions that change the CPU count and the amount of memory, you must consider several factors to determine if you want to use the Power Off Allowed option. These factors include whether you are increasing or decreasing the CPU or memory and whether the target virtual machines are powered on. If you increasing the CPU or memory values, whether hot plug is enabled also affects how you apply the option when you run the action.

How you use Power Off Allowed when you are decreasing the CPU count or the amount of memory depends on the power state of the target virtual machines.

**Table 2-4. Decreasing CPU Count and Memory Behavior Based On Options**

Virtual Machine Power State	Power Off Allowed Selected	Results
On	Yes	If VMware Tools is installed and running, the action shuts down the virtual machine, decreases the CPU or memory, and powers the machine back on.  If VMware Tools is not installed, the action powers off the virtual machine, decreases the CPU or memory, and powers the machine back on.
On	No	The action does not run on the virtual machine.
Off	Not applicable. The virtual machine is powered off.	The action decreases the value and leaves the virtual machine in a powered off state.

How you use Power Off Allowed when you are increasing the CPU count or the amount of memory depends on several factors, including the state of the target virtual machine and whether hot plug is enabled. Use the following information to determine which scenario applies to your target objects.

If you are increasing the CPU count, you must consider the power state of the virtual machine and whether CPU Hot Plug is enabled when determining whether to apply Power Off Allowed.

**Table 2-5. Increasing CPU Count Behavior.**

Virtual Machine Power State	CPU Hot Plug Enabled	Power Off Allowed Selected	Results
On	Yes	No	The action increases the CPU count to the specified amount.
On	No	Yes	If VMware Tools is installed and running, the action shuts down the virtual machine, increases the CPU count, and powers the machine back on.  If VMware Tools is not installed, the action powers off the virtual machine, increases the CPU count, and powers the machine back on.
Off	Not applicable. The virtual machine is powered off.	Not required.	The action increases the CPU count to the specified amount.

If you are increasing the memory, you must consider the power state of the virtual machine, whether Memory Hot Plug is enabled, and whether there is a Hot Memory Limit when determining how to apply Power Off Allowed.

**Table 2-6. Increasing Memory Amount Behavior**

<b>Virtual Machine Power State</b>	<b>Memory Hot Plug Enabled</b>	<b>Hot Memory Limit</b>	<b>Power Off Allowed Selected</b>	<b>Results</b>
On	Yes	New memory value $\leq$ hot memory limit	No	The action increases the memory the specified amount.
On	Yes	New memory value $>$ hot memory limit	Yes	<p>If VMware Tools is installed and running, the action shuts down the virtual machine, increases the memory, and powers the machine back on.</p> <p>If VMware Tools is not installed, the action powers off the virtual machine, increases the memory, and powers the machine back on.</p>
On	No	Not applicable. The hot plug is not enabled.	Yes	<p>If VMware Tools is installed and running, the action shuts down the virtual machine, increases the memory, and powers the machine back on.</p> <p>If VMware Tools is not installed, the action powers off the virtual machine, increases the memory, and powers the machine back on.</p>
Off	Not applicable. The virtual machine is powered off.	Not applicable.	Not required	The action increases the memory the specified amount.

# Configuring Policies

To create a new policy, you can inherit the settings from an existing policy, and you can modify the settings in existing policies if you have adequate permissions. After you create a new policy, or edit an existing policy, you can apply the policy to one or more groups of objects

This chapter includes the following topics:

- [Policies](#)
- [Operational Policies](#)
- [Types of Policies](#)
- [Using the Monitoring Policy Workspace to Create and Modify Operational Policies](#)

## Policies

A policy is a set of rules that you define for vRealize Operations Manager to use to analyze and display information about the objects in your environment. You can create, modify, and administer policies to determine how vRealize Operations Manager displays data in dashboards, views, and reports.

## How Policies Relate to Your Environment

vRealize Operations Manager policies support the operational decisions established for your IT infrastructure and business units. With policies, you control what data vRealize Operations Manager collects and reports on for specific objects in your environment. Each policy can inherit settings from other policies, and you can customize and override various analysis settings, alert definitions, and symptom definitions for specific object types, to support the service Level agreements and business priorities established for your environment.

When you manage policies, you must understand the operational priorities for your environment, and the tolerances for alerts and symptoms to meet the requirements for your business critical applications. Then, you can configure the policies so that you apply the correct policy and threshold settings for your production and test environments.

Policies define the settings that vRealize Operations Manager applies to your objects when it collects data from your environment. vRealize Operations Manager applies policies to newly discovered objects, such as the objects in an object group. For example, you have an existing VMware adapter instance, and you apply a specific policy to the group named World. When a user adds a new virtual machine to the vCenter Server instance, the VMware adapter reports the virtual machine object to vRealize Operations Manager. The VMware adapter applies the same policy to that object, because it is a member of the World object group.

To implement capacity policy settings, you must understand the requirements and tolerances for your environment, such as CPU use. Then, you can configure your object groups and policies according to your environment.

- For a production environment policy, a good practice is to configure higher performance settings, and to account for peak use times.
- For a test environment policy, a good practice is to configure higher utilization settings.

vRealize Operations Manager applies policies in priority order, as they appear on the Active Policies tab. When you establish the priority for your policies, vRealize Operations Manager applies the configured settings in the policies according to the policy rank order to analyze and report on your objects. To change the priority of a policy, you click and drag a policy row. The default policy is always kept at the bottom of the priority list, and the remaining list of active policies starts at priority 1, which indicates the highest priority policy. When you assign an object to be a member of multiple object groups, and you assign a different policy to each object group, vRealize Operations Manager associates the highest ranking policy with that object.

**Table 3-1. Configurable Policy Rule Elements**

Policy Rule Elements	Thresholds, Settings, Definitions
Workload	Enable or disable the demand for memory, CPU, and disk space. Enable or disable the rates for network I/O and datastore I/O, and set the vSphere configuration limit. Configure symptom thresholds for the Workload badge score.
Anomalies	Configure symptom thresholds for the Anomalies badge score.
Faults	Configure symptom thresholds for the Faults badge score.
Capacity Remaining and Time Remaining	Enable or disable the demand and allocation for memory, CPU, and disk space. Enable or disable the rates for network I/O and datastore I/O, and set the vSphere configuration limit. Account for peak times, account for committed projects, which affect the time remaining, and set the provisioning time buffer. Configure thresholds for the Capacity and Time Remaining badge scores.
Stress	Enable or disable the demand for memory and CPU. Enable or disable the rates for network I/O and datastore I/O, and set the vSphere configuration limit. Configure symptom thresholds for the stress badge score.
Reclaimable Capacity	Set the recommended oversize percentage, and the idle and powered off time percentages. Configure symptom thresholds for the Reclaimable Capacity badge score.
Density	Configure symptom thresholds for the Density badge score.
Time	Track the use of objects, and select the maintenance schedule.

Policy Rule Elements	Thresholds, Settings, Definitions
Attributes	<p>An attribute is a collectible data component. You can enable or disable metric, property, and super metric attributes for collection, and set attributes as key performance indicators (KPIs). A KPI is the designation of an attribute that indicates that the attribute is important in your own environment.</p> <p>vRealize Operations Manager treats KPIs differently from other attributes. Threshold violations by a KPI generate different types of alerts from non-KPI attributes.</p> <p>When a KPI violates a threshold, vRealize Operations Manager examines the events that preceded the violation. If it finds enough related information, vRealize Operations Manager captures the set of events that preceded the violation as a fingerprint. If it finds a similar series of events in the future, it can issue a predictive alert warning that the KPI violation is likely to occur.</p>
Alert Definitions	Enable or disable combinations of symptoms and recommendations to identify a condition that classifies as a problem.
Symptom Definitions	Enable or disable test conditions on properties, metrics, or events.

## Privileges To Create, Modify, and Prioritize Policies

You must have privileges to access specific features in the vRealize Operations Manager user interface. The roles associated with your user account determine the features you can access and the actions you can perform.

To set the policy priority, on the Active Policies tab, click the policy row and drag it to place it at the desired priority in the list. The priority for the Default Policy is always designated with the letter D.

## How Upgrades Affect Your Policies

After you upgrade vRealize Operations Manager from a previous version, you might find newly added or updated default settings of policies such as, new alerts and symptoms. Hence, you must analyze the settings and modify these settings to optimize them for your current environment. If you apply the policies used with a previous version of vRealize Operations Manager, the manually modified policy settings remain unaltered.

## Policy Decisions and Objectives

Implementing policy decisions in vRealize Operations Manager is typically the responsibility of the Infrastructure Administrator or the Virtual Infrastructure Administrator, but users who have privileges can also create and modify policies.

You must be aware of the policies established to analyze and monitor the resources in your IT infrastructure.

- As a Virtual Infrastructure Administrator who manages and troubleshoots an IT infrastructure, you must understand how policies associated with objects affect the scores that appear in vRealize Operations Manager, so that you can configure the approved policies based on your company decisions and requirements.
- If you are a Network Operations engineer, you must understand how policies affect the data that vRealize Operations Manager reports on objects, and which policies assigned to objects report alerts and issues.

- If you are the person whose role is to recommend an initial setup for policies, you typically edit and configure the policies in vRealize Operations Manager.
- If your primary role is to assess problems that occur in your environment, but you do not have the responsibility to change the policies, you must still understand how the policies applied to objects affect the data that appears in vRealize Operations Manager. For example, you might need to know which policies apply to objects that are associated with particular alerts.
- If you are a typical application user who receives reports from vRealize Operations Manager, you must have a high-level understanding of the operational policies so that you can understand the reported data values.

## Policy Library Tab for Policies

The **Policy Library** tab displays the base settings, default policy, and other best practice policies that vRealize Operations Manager includes. You can use the library policies to create your own policies. The policy library includes all of the configurable settings for the policy elements, such as workload, anomaly, faults, capacity and time remaining, stress, reclaimable capacity, density, usable capacity, and time.

### How the Policy Library Works

Use the options on the **Policy Library** tab to create your own policy from an existing policy, or to override the settings from an existing policy so that you can apply the new settings to groups of objects. You can also import and export a policy.

To display the details for a selected policy, click the split bar to expand the pane. The Details and Related Items tabs and options for the policy appear in the lower pane. On the Related Items tab, you can also apply the selected policy to object groups.

When you add or edit a policy, you access the policy workspace where you select the base policies and override the settings for analysis, metrics, properties, alert definitions, and symptom definitions. In this workspace, you can also apply the policy to object groups. To update the policy association with an object group, the role assigned to your user account must have the Manage Association permission enabled for policy management.

### Where You Manage the Policy Library

To manage the policy library, click **Administration** and click **Policies**. The **Policy Library** tab appears and lists the policies available to use for your environment.

**Table 3-2. Policy Library Tab Options**

Option	Description
Toolbar	<p>Use the toolbar selections to take action in the policy library.</p> <ul style="list-style-type: none"> <li>■ Add New Policy. Create a policy from an existing policy.</li> <li>■ Edit Selected Policy. Customize the policy so that you can override settings for vRealize Operations Manager to analyze and report data about the associated objects.</li> <li>■ Set Default Policy. You can set any policy to be the default policy, which applies the settings in that policy to all objects that do not have a policy applied. When you set a policy to be the default policy, the priority is set to 0, which gives that policy the highest priority.</li> <li>■ Import Policy and Export Policy. You can import or export a policy in XML format. To import or export a policy, the role assigned to your user account must have the Import or Export permissions enabled for policy management.</li> <li>■ Delete Selected Policy. Remove a policy from the list.</li> </ul>
Policy Library Tab data grid	<p>vRealize Operations Manager displays the high-level details for the policies.</p> <ul style="list-style-type: none"> <li>■ Name. Name of the policy as it appears in the Add or Edit Monitoring Policy wizard, and in areas where the policy applies to objects, such as in Custom Groups.</li> <li>■ Description. Meaningful description of the policy, such as which policy is inherited, and any specific information users need to understand the relationship of the policy to one or more groups of objects.</li> <li>■ Last Modified. Date and time that the policy was last modified.</li> <li>■ Modified By. User who last modified the policy settings.</li> </ul>

Option	Description
Policy Library Tab > Details Tab	<p>The Details tab displays the name and description of the policy from which the settings are inherited, the policy priority, who last modified the policy, and the number of object groups associated with the policy. From the Details tab, you can view the settings that are locally defined in your policy, and the complete group of settings that include both customized settings and the settings inherited from the base policies selected when the policy was created.</p> <ul style="list-style-type: none"> <li>■ <b>Locally Defined Settings.</b> Displays the locally changed policy element settings for each object type in the policy. For example, if you changed the Memory Demand settings in the Cluster Compute Object Stress policy element, you can see the update to your local policy in the list of locally defined settings.</li> <li>■ <b>Complete Settings Including Inherited.</b> Displays all of the policy element settings for each object type in the policy, including locally changed settings and settings that are inherited. A summary of the enabled and disabled alert definitions, symptom definitions, and attributes appear indicate the number of changes in the policy. The policy element settings include badge score symptom thresholds, and indicate changes made to the Workload, Anomaly, Fault, Capacity and Time Remaining, Stress, Reclaimable Capacity, Density, Usable Capacity, and Time settings. For example, if you changed the Cluster Compute Object Usable Capacity policy element settings, you can see the updates to your local policy in the complete list of settings, and the high availability configuration setting. If you have various adapters installed, such as the vRealize Configuration Manager Adapter, you will also see specific policy elements for the adapter. For example, for vRealize Configuration Manager you will see the Compliance policy element setting and badge score symptom threshold.</li> </ul>
Related ObjectsTab	<p>Summarizes the related groups and objects, and details about the selected object group and objects.</p> <ul style="list-style-type: none"> <li>■ <b>Groups.</b> Displays the groups of objects associated with the selected active policy, and provides options to add and release an association. <ul style="list-style-type: none"> <li>■ <b>Add Association.</b> Opens the Apply the policy to groups dialog box where you select object groups to associate with the selected policy.</li> <li>■ <b>Release Association.</b> Opens a confirmation dialog box to confirm the release of the object group that is associated with the selected policy.</li> <li>■ <b>Data grid.</b> Displays the groups assigned to this policy, the object types associated with the group, and the number of objects in the group.</li> <li>■ <b>Details for the selected object group.</b> Displays the object group name, type, and number of members associated with the selected policy, and the type of association with the policy. An object group can have a direct association with a policy, and inherited policy associations based on the base policies that you selected when you created a local policy. For example, if the Base Settings policy appears in the list, with an inherited association, the Base Settings policy was included in the base policies selected when this policy was created.</li> </ul> </li> <li>■ <b>Affected Objects.</b> Displays the names of the objects in your environment, their object types, and associated adapters. When a parent group exists for an object, it appears in this data grid.</li> </ul>

## Active Policies Tab for Policies

The **Active Policies** tab displays the policies associated with groups of objects. You can manage the active policies for the objects in your environment so that you can have vRealize Operations Manager analyze and display specific data about those objects in dashboards, views, and reports.

## How the Active Policies Tab Works

Use the **Active Policies** tab to associate a policy with one or more object groups, and to set the default policy. You can view the locally defined settings for a policy, and the complete list of settings, which includes those that are inherited from the base policies that you select in the Add or Edit Policy workspace. You can assign any policy to be the default policy.

vRealize Operations Manager applies policies in priority order, as they appear on the Active Policies tab. When you establish the priority for your policies, vRealize Operations Manager applies the configured settings in the policies according to the policy rank order to analyze and report on your objects. To change the priority of a policy, you click and drag a policy row. The default policy is always kept at the bottom of the priority list, and the remaining list of active policies starts at priority 1, which indicates the highest priority policy. When you assign an object to be a member of multiple object groups, and you assign a different policy to each object group, vRealize Operations Manager associates the highest ranking policy with that object.

To display the details for a selected policy, click the split bar to expand the pane. The Details and Related Items tabs and options for the policy appear in the lower pane. On the Related Items tab, you can also apply the selected policy to object groups.

You can use the far right column of the **Active Policies** tab to reorder and therefore reprioritize the policies by dragging them to a new position. However, even though it seems like you can drag a custom policy below the default policy, you cannot. The default policy is always the last policy in the list after the view is refreshed.

## How to Prioritize Policies

To set the policy priority, on the Active Policies tab, click the policy row and drag it to place it at the desired priority in the list. The priority for the Default Policy is always designated with the letter D.

## Where You Manage the Active Policies

To manage the active policies, click **Administration** and click **Policies**. The **Active Policies** tab appears and lists the policies that are active for the objects in your environment.

**Table 3-3. Active Policies Tab Options**

Option	Description
Toolbar	<p>Use the toolbar selections to take action on the active policies.</p> <ul style="list-style-type: none"> <li>■ Add Association. Opens the <b>Related Items</b> tab so that you can associate the policy with groups.</li> <li>■ Set Default Policy. You can set any policy to be the default policy, which applies the settings in that policy to all objects that do not have a policy applied. When you set a policy to be the default policy, the priority is set to D, which gives that policy the highest priority.</li> </ul>
Active Policies Tab data grid	<p>vRealize Operations Manager displays the priority and high-level details for the active policies.</p> <ul style="list-style-type: none"> <li>■ Priority. Ranking of the priority of the policy. The default policy is marked with a check mark in the Is Default column.</li> <li>■ Name. Name of the policy as it appears in the Add or Edit Monitoring Policy wizard, and in areas where the policy applies to objects, such as in Custom Groups.</li> <li>■ Description. Meaningful description of the policy, such as which policy is inherited, and any specific information users need to understand the relationship of the policy to one or more groups of objects.</li> <li>■ Groups. Indicates the number of object groups to which the policy is assigned.</li> <li>■ Affected Objects. Displays the object name, type, and adapter to which the active policy is assigned, and the direct parent group, when applicable.</li> <li>■ Last Modified. Date and time that the policy was last modified.</li> <li>■ Modified By. User who last modified the policy settings.</li> </ul>

Option	Description
Active Policies Tab > Details Tab	<p>The Details tab displays the name and description of the policy from which the settings are inherited, the policy priority, who last modified the policy, and the number of object groups associated with the policy. From the Details tab, you can view the settings that are locally defined in your policy, and the complete group of settings that include both customized settings and the settings inherited from the base policies selected when the policy was created.</p> <ul style="list-style-type: none"> <li>■ <b>Locally Defined Settings.</b> Displays the locally changed policy element settings for each object type in the policy. For example, if you changed the Memory Demand settings in the Cluster Compute Object Stress policy element, you can see the update to your local policy in the list of locally defined settings.</li> <li>■ <b>Complete Settings Including Inherited.</b> Displays all of the policy element settings for each object type in the policy, including locally changed settings and settings that are inherited. A summary of the enabled and disabled alert definitions, symptom definitions, and attributes appear indicate the number of changes in the policy. The policy element settings include badge score symptom thresholds, and indicate changes made to the Workload, Anomaly, Fault, Capacity and Time Remaining, Stress, Reclaimable Capacity, Density, Usable Capacity, and Time settings. For example, if you changed the Cluster Compute Object Usable Capacity policy element settings, you can see the updates to your local policy in the complete list of settings, and the high availability configuration setting. If you have various adapters installed, such as the vRealize Configuration Manager Adapter, you will also see specific policy elements for the adapter. For example, for vRealize Configuration Manager you will see the Compliance policy element setting and badge score symptom threshold.</li> </ul>
Active Policies Tab > Related Objects Tab	<p>Summarizes the related groups and objects, and details about the selected object group and objects.</p> <ul style="list-style-type: none"> <li>■ <b>Groups.</b> Displays the groups of objects associated with the selected active policy, and provides options to add and release an association. <ul style="list-style-type: none"> <li>■ <b>Add Association.</b> Opens the Apply the policy to groups dialog box where you select object groups to associate with the selected policy.</li> <li>■ <b>Release Association.</b> Opens a confirmation dialog box to confirm the release of the object group that is associated with the selected policy.</li> <li>■ <b>Data grid.</b> Displays the groups assigned to this policy, the object types associated with the group, and the number of objects in the group.</li> <li>■ <b>Details for the selected object group.</b> Displays the object group name, type, and number of members associated with the selected policy, and the type of association with the policy. An object group can have a direct association with a policy, and inherited policy associations based on the base policies that you selected when you created a local policy. For example, if the Base Settings policy appears in the list, with an inherited association, the Base Settings policy was included in the base policies selected when this policy was created.</li> </ul> </li> <li>■ <b>Affected Objects.</b> Displays the names of the objects in your environment, their object types, and associated adapters. When a parent group exists for an object, it appears in this data grid.</li> </ul>

## Operational Policies

Determine how to have vRealize Operations Manager monitor your objects, and how to notify you about problems that occur with those objects.

vRealize Operations Manager Administrators assign policies to object groups and applications to support Service Level Agreements (SLAs) and business priorities. When you use policies with object groups, you ensure that the rules defined in the policies are quickly put into effect for the objects in your environment.

With policies, you can:

- Enable and disable alerts.
- Control data collections by persisting or not persisting metrics on the objects in your environment.
- Configure the product analytics and thresholds.
- Monitor objects and applications at different service levels.
- Prioritize policies so that the most important rules override the defaults.
- Understand the rules that affect the analytics.
- Understand which policies apply to object groups.

vRealize Operations Manager includes a library of built-in active policies that are already defined for your use. vRealize Operations Manager applies these policies in priority order.



Create Operational Policies

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_create\\_policies\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_create_policies_vrom))

When you apply a policy to an object group, vRealize Operations Manager collects data from the objects in the object group based on the thresholds, metrics, super metrics, attributes, properties, alert definitions, and problem definitions that are enabled in the policy.

The following examples of policies might exist for a typical IT environment.

- Maintenance: Optimized for ongoing monitoring, with no thresholds or alerts.
- Critical Production: Production environment ready, optimized for performance with sensitive alerting.
- Important Production: Production environment ready, optimized for performance with medium alerting.
- Batch Workloads: Optimized to process jobs.
- Test, Staging, and QA: Less critical settings, fewer alerts.
- Development: Less critical settings, no alerts.
- Low Priority: Ensures efficient use of resources.
- Default Policy: Default system settings.

## User Scenario: Create an Operational Policy for Production vCenter Server Datastore Objects

As a Virtual Infrastructure Administrator, you manage the policies used for vRealize Operations Manager to analyze objects in your environment, collect data from those objects, and display that data in dashboards, views, and reports. Your IT staff added new datastore objects to your environment, and your

responsibility is to ensure that the new datastore objects adhere to the policy requirements from the VP of Infrastructure for your test and production environments.

In this scenario, you create a policy to have vRealize Operations Manager monitor the disk space use of your production datastore objects. You create a group type and custom object group for the datastore objects, and apply your policy to your object group. After vRealize Operations Manager collects data from the datastore objects in your environment according to the settings in your policy, you view the collected data and any potential alerts in the dashboards to confirm whether the disk space use is in compliance for your datastore objects.

### Prerequisites

- Understand the purpose of using a policy. See [Policies](#) .
- Verify that your vRealize Operations Manager instance is working properly.
- Verify that one or more custom object groups and group types exist in your vRealize Operations Manager instance. See [Managing Custom Object Groups in VMware vRealize Operations Manager](#).
- Verify that your vRealize Operations Manager instance includes the default policy and one or more other policies. See [Default Policy in vRealize Operations Manager](#).
- Understand the sections and elements in the default policy, such as the attributes, alert and symptom definitions, and how the policy inherits settings from the base policies that you select. See [Policy Workspace in vRealize Operations Manager](#).
- Understand the analysis settings in the default policy, such as capacity remaining and stress on hosts and virtual machines, and the actions used to override the settings inherited from the base policies. See the vRealize Operations Manager Information Center.

### Procedure

- 1 [Create a Group Type for Your Datastore Objects](#)  
Create a group type so that you can categorize your Datastore objects.
- 2 [Create an Object Group for Your Datastore Objects](#)  
Create an object group to organize the Datastore objects in your environment as a single object group.
- 3 [Create Your Policy and Select a Base Policy](#)  
Create your policy, and select the base policies to use to override the settings for your new policy.
- 4 [Override the Analysis Settings for the Datastore Objects](#)  
Display and override the analysis settings for the Datastore objects that your new policy will monitor.
- 5 [Enable Disk Space Attributes for Datastore Objects](#)  
Enable the attributes for vRealize Operations Manager to monitor the disk space of your production datastore objects.
- 6 [Override Alert and Symptom Definitions for Datastore Objects](#)  
Override the alert and symptom definitions for Datastore objects.

## 7 Apply Your Datastore Policy to Your Datastore Objects Group

Apply the policy to your new group of Datastore objects to have vRealize Operations Manager monitor them to ensure that the disk space levels of these objects adhere to the settings in your policies to support the service level agreements and business priorities that are established for your environment.

## 8 Create a Dashboard for Disk Use of Your Datastore Objects

Create a dashboard so that you can monitor the disk use of your Datastore objects, and be alerted to any potential problems.

You created a policy to apply to your new production Datastore objects so that you can have vRealize Operations Manager monitor them to ensure that the disk space levels of these objects adhere to the settings in your policies to support the service level agreements and business priorities that are established for your environment. vRealize Operations Manager uses the settings in your new policy to display the disk use for your Datastore objects in dashboards, views, and reports, and to enforce the service levels during data collections.

### What to do next

After you finish this scenario, you must wait for vRealize Operations Manager to collect data from the objects in your environment. Then view the disk use of your Datastore objects.

## Create a Group Type for Your Datastore Objects

Create a group type so that you can categorize your Datastore objects.

In this step, you create a group type so that you can apply it to the new custom object group that you will create to organize your vCenter Server Datastore objects.

### Prerequisites

Verify that you understand the context of this scenario. See [User Scenario: Create an Operational Policy for Production vCenter Server Datastore Objects](#).

### Procedure

- 1 In the navigation pane, click **Content** and click **Group Types**.
- 2 Click the plus sign to add a new group type, type **Production\_Datastores**, and click **OK**.

The new group type appears in the list of group types.

### What to do next

Create an object group so that you can organize the Datastore objects in your environment as a single object group.

## Create an Object Group for Your Datastore Objects

Create an object group to organize the Datastore objects in your environment as a single object group.

In this step, you create a new object group to organize your Datastore objects so that you can apply the policy that you create to the object group.

### Prerequisites

Create an object type. See [Create a Group Type for Your Datastore Objects](#).

### Procedure

- 1 Select **Environment**, and click **Custom Groups**.
- 2 On the **Groups** tab, click the plus sign to add a new group, and enter a name for the object group.
- 3 From the **Group Type** drop-down menu, select your new group type.
- 4 From the **Policy** drop-down menu, select the Default Policy for now.
 

To have vRealize Operations Manager identify new Datastore objects that are added to your environment, you select the **Keep group membership up to date** check box to make this group dynamic and keep it updated.
- 5 In the Define membership criteria pane, select the **vCenter Adapter > Datastore** object type from the drop-down menu.
- 6 Click in the **Pick a property** text box, and select **Disk Space > Template > Virtual Machine used (GB)**.
- 7 In the adjacent text box, click the drop-down arrow and select **is less than**.
- 8 In the **Property value** text box, type **10**.
 

vRealize Operations Manager uses this criteria to monitor Datastore objects in this group, and to report when the Datastore objects have less than 10 GB of space remaining.
- 9 In the Objects to always include pane, select the object group that you created for your Datastore objects, click **Add** to move the group to the selected pane, and select the object group check box.
 

In the Objects to always exclude pane, do not select objects to exclude.
- 10 Click **OK** to save your new group.

### What to do next

Create your policy, and select the base policies to use to override the settings for your new policy.

## Create Your Policy and Select a Base Policy

Create your policy, and select the base policies to use to override the settings for your new policy.

In this step, you create a policy for vRealize Operations Manager to analyze and monitor your Datastore objects, and select the policies from which to inherit and override the settings for your new policy.

### Prerequisites

Create a custom object group for your Datastore objects. See [Create an Object Group for Your Datastore Objects](#).

## Procedure

- 1 Access the Policies area to create your policy.
  - a Click **Administration**, and click **Policies**.  
The **Active Policies** and **Policy Library** tabs appear.
  - b Click the **Policy Library** tab, and click the plus sign to add a policy.
  - c In the Getting Started policy workspace, enter a name and description for the policy.
  - d In the Start with area, select **Default Policy** to inherit settings from a base policy.
- 2 Select the base policies, object, and policy to use to override the settings for your new policy.
  - a In the policy workspace, click **Select Base Policies**.
  - b To view the current policy configuration for your Datastore objects, click the **Show changes for** drop-down menu, click **vCenter Adapter - Datastore**, and click the **Show object type** filter.  
The Datastore policy configuration appears in the right pane.

## What to do next

Display and override the analysis settings for the Datastore objects that your new policy will monitor.

## Override the Analysis Settings for the Datastore Objects

Display and override the analysis settings for the Datastore objects that your new policy will monitor.

In this step, you override the capacity remaining and time remaining settings for your new policy, and override the capacity score symptom thresholds so that vRealize Operations Manager triggers an alert and notifies you of potential problems with the capacity of your Datastore objects.

## Prerequisites

Create your policy and select the base policies to inherit and override the settings for your new policy. See [Create Your Policy and Select a Base Policy](#).

## Procedure

- 1 In the policy workspace, click **Analysis Settings**.
- 2 Click the **Show changes for** drop-down menu, click **vCenter Adapter - Datastore**, and click the **Show object type** filter.  
The vCenter Adapter - Datastore object type appears in the Object types list, and the analysis settings for Datastore objects appear in the right pane. The policy elements include thresholds and settings for all of the analysis capabilities, such as Workload, Stress, Usable Capacity, and so on.
- 3 Click the policy element override button for the Capacity Remaining and Time Remaining element to turn on this policy element.  
The button changes to a check mark, and the policy element becomes active so that you can override the settings.

- 4 Click and drag the settings on the Capacity Score Symptom Threshold slider to 10% for warning (red), 15% for caution (orange), and 20% for normal (green).

When these thresholds are violated for the Datastore objects in your environment, vRealize Operations Manager triggers an alert and notifies you of a potential problem with the capacity of your Datastore objects.

- 5 Click the policy element override button for the Usable Capacity element to turn on this policy element, click the arrow to expand the policy element view, and select the **Use High Availability (HA) Configuration** check box.

When you use High Availability, you ensure that vRealize Operations Manager provides enough resources for your Datastore objects to handle throughput and potential loss of data.

### What to do next

Enable the disk space attributes for datastore objects.

## Enable Disk Space Attributes for Datastore Objects

Enable the attributes for vRealize Operations Manager to monitor the disk space of your production datastore objects.

In this step, you enable vRealize Operations Manager to monitor and collect the disk space properties attribute from the Datastore objects in your environment.

### Prerequisites

Override the analysis settings for your Datastore objects. See [Override the Analysis Settings for the Datastore Objects](#).

### Procedure

- 1 In the policy workspace, click **Override Attributes**.
- 2 From the Object Type drop-down menu, select **vCenter Adapter > Datastore**.  
vRealize Operations Manager filters the list and displays only the attributes that apply to Datastore objects.
- 3 Click the **Attribute Type** drop-down menu, select **Property**, and deselect the other attributes.
- 4 Enter **space** in the **Search** text box, and click the search button.  
vRealize Operations Manager filters the list and displays only the disk space properties associated with Datastore objects.
- 5 For the **Disk Space|Template|Virtual Machine used (GB)** property attribute, click the **State** drop-down menu, and click **Local**.

When this attribute is enabled in your local policy, vRealize Operations Manager collects this disk space properties attribute from Datastore objects in your environment.

**What to do next**

Override the alert symptom definitions for Datastore objects.

**Override Alert and Symptom Definitions for Datastore Objects**

Override the alert and symptom definitions for Datastore objects.

In this step, you override the alert and symptom definitions so that vRealize Operations Manager uses trigger an alert notification during data collections when the disk space for your Datastore objects begins to run out.

**Prerequisites**

Enable vRealize Operations Manager to monitor and collect the disk space properties attribute from the Datastore objects in your environment. See [Enable Disk Space Attributes for Datastore Objects](#).

**Procedure**

- 1 In the policy workspace, click **Alert / Symptom Definitions**.
- 2 In the Alert Definitions pane, from the Object Type drop-down menu, select **vCenter Adapter > Datastore**.
- 3 Enter **space** in the **Search** text box, and click the search button.
- 4 For the alert definition named *Datastore is running out of disk space*, click the **State** drop-down menu and click **Local**.

When this alert definition is enabled in your local policy, vRealize Operations Manager uses it to trigger an alert notification during data collections when the disk space for your Datastore objects begins to run out.

- 5 In the Symptom Definitions pane, from the Object Type drop-down menu, select **vCenter Adapter > Datastore**.
- 6 Enter **space** in the **Search** text box, and click the search button.
- 7 To enable the critical, immediate, and warning symptom definitions for the space use on datastore objects, click **Actions**, and click **Select All**, then set the thresholds.

**Table 3-4. Symptom Definitions Threshold Settings**

<b>Selection</b>	<b>Setting</b>
Datastore space use reaching critical limit	>90
Datastore space use reaching immediate limit	>85
Datastore space use reaching warning limit	>80

**What to do next**

Apply your policy to your Datastore objects.

## Apply Your Datastore Policy to Your Datastore Objects Group

Apply the policy to your new group of Datastore objects to have vRealize Operations Manager monitor them to ensure that the disk space levels of these objects adhere to the settings in your policies to support the service level agreements and business priorities that are established for your environment.

In this step, you apply your new policy to production Datastore objects so that vRealize Operations Manager monitors them to ensure adequate disk space levels of these objects.

### Prerequisites

Override the alert and symptom definitions for Datastore objects. See [Override Alert and Symptom Definitions for Datastore Objects](#).

### Procedure

- 1 In the policy workspace, click **Apply Policy to Groups**, and select the new object group that you created for your Datastore objects.
- 2 Click **Save** to save your new policy settings.

vRealize Operations Manager uses the settings in your new policy to display the disk use for your Datastore objects in dashboards, views, and reports, and to enforce the service levels during data collections

### What to do next

Create a new dashboard to view the disk use of your Datastore objects.

## Create a Dashboard for Disk Use of Your Datastore Objects

Create a dashboard so that you can monitor the disk use of your Datastore objects, and be alerted to any potential problems.

In this step, you create a new dashboard, add widgets to your new dashboard, and configure the widgets so that you can monitor your production datastore objects.

### Prerequisites

Apply the policy to your new group of Datastore objects. See [Apply Your Datastore Policy to Your Datastore Objects Group](#).

### Procedure

- 1 Click **Home**.
- 2 Click **Actions > Create a Dashboard**.
- 3 Configure your new dashboard.
  - a In the Dashboard Configuration pane of the New Dashboard workspace, enter the name **Production Datastores** for the new dashboard.
  - b For Is default, select **Yes**.

- 4 Add widgets to your new dashboard.
  - a In the workspace, click **Widget List**.
  - b From the list of widgets, click the **Object List** widget, and drag it to the right pane.
  - c Click the **Capacity** widget, and drag it to the right pane.
  - d Click the **Time Remaining** widget, and drag it to the right pane.
  - e Click the **Alert List** widget, and drag it to the right pane.
- 5 Configure the widget interactions.
  - a In the workspace, click **Widget Interactions**.
  - b For the Object List widget interactions, click the drop-down menu for the Selected Objects and Selected Alerts, and clear the selections.
  - c For the Alert List widget interaction, click the drop-down and select **Object List**.
  - d For the Capacity widget interaction, click the drop-down and select **Object List**.
  - e For the Time Remaining widget interaction, click the drop-down and select **Object List**.
  - f Click **Apply Interactions**.
- 6 Configure the Object List widget.
  - a On the Object List widget, click the pencil.
  - b For Refresh Content, select **On**.
  - c For Refresh Interval, click the arrows and select **30** seconds.
  - d For Mode, select **Parent**.
  - e For Auto Select First Row, select **Off**.
  - f In the lower pane, click the plus sign to expand the list of tags, expand **Production Datastores**, select **Production Datastores (n)**, and click **OK**.

The objects in your Production Datastores object group appears in the Object List widget.

- 7 Configure the Capacity widget.
  - a On the Capacity widget, click the pencil.
  - b For Refresh Content, select **On**.
  - c For Refresh Interval, click the arrows and select **30** seconds.
  - d For Self Provider, select **On**.
  - e For Selected Object, in the **Search** text box, enter **group**, and select the **Production Datastores** group from the list.

The Production Datastores group appears in the **Selected Object** text box.
  - f Click **OK**.

The Capacity widget displays a score and a graph to indicate the remaining compute objects as a percentage of the total consumer capacity.

## 8 Configure the Time Remaining widget.

- a On the Time Remaining widget, click the pencil.

The Time Remaining widget displays the amount of time that remains until the object resources are consumed.

- b For Refresh Content, select **On**.

The Time Remaining widget displays the amount of time that remains until the object resources are consumed.

- c For Refresh Interval, click the arrows and select **30** seconds.

- d For Self Provider, select **On**.

- e For Selected Object, in the **Search** text box, enter **group**, and select the **Production Datastores** group from the list.

The Production Datastores group appears in the **Selected Object** text box.

- f Click **OK**.

The Time Remaining widget displays a score and a graph to indicate the amount of time that remains until the object resources are consumed.

## 9 Configure the Alert List widget.

- a On the Alert List widget, click the pencil.

- b For Refresh Content, select **On**.

- c For Refresh Interval, click the arrows and select **30** seconds.

- d For Selected Object, in the **Search** text box, enter **group**, and select the **Production Datastores** group from the list.

The Production Datastores group appears in the **Selected Object** text box.

- e In the lower pane, click the plus sign to expand the list of tags, expand **Production Datastores**, select **Production Datastores (n)**, and click **OK**.

The alert list widget displays the alerts that are configured for your objects. You created a dashboard to monitor disk space of your production datastore objects. After vRealize Operations Manager analyzes and collects data from the objects in your Production Datastores object group, you can view the results in your new dashboard.

You created and applied a policy to your production datastore objects to have vRealize Operations Manager monitor those objects during data collections so that you can monitor and enforce the service levels for your environment. vRealize Operations Manager uses the settings in your new policy to display information about the capacity, time remaining, and potential alerts for your Datastore objects. With your new policy in place, you can ensure that the disk space levels for your production datastore objects adhere to the policies established for your production environment.

## Types of Policies

There are three types of policies such as default policies, custom policies, and policies that are offered with vRealize Operations Manager.

### Custom Policies

You can customize the default policy and base policies included with vRealize Operations Manager for your own environment. You can then apply your custom policy to groups of objects, such as the objects in a cluster, or virtual machines and hosts, or to a group that you create to include unique objects and specific criteria.

You must be familiar with the policies so that you can understand the data that appears in the user interface, because policies drive the results that appear in the vRealize Operations Manager dashboards, views, and reports.

To determine how to customize operational policies and apply them to your environment, you must plan ahead. For example:

- Must you track CPU allocation? If you overallocate CPU, what percentage must you apply to your production and test objects?
- Will you overallocate memory or storage? If you use High Availability, what buffers must you use?
- How do you classify your logically defined workloads, such as production clusters, test or development clusters, and clusters used for batch workloads? Or, do you include all clusters in a single workload?
- How do you capture peak use times or spikes in system activity? In some cases, you might need to reduce alerts so that they are meaningful when you apply policies.

When you have privileges applied to your user account through the roles assigned, you can create and modify policies, and apply them to objects. For example:

- Create a policy from an existing base policy, inherit the base policy settings, then override specific settings to analyze and monitor your objects.
- Use policies to analyze and monitor vCenter Server objects and non-vCenter Server objects.
- Set custom thresholds for analysis settings on all object types to have vRealize Operations Manager report on workload, anomalies, faults, capacity, stress, and so on.
- Enable specific attributes for collection, including metrics, properties, and super metrics.
- Enable or disable alert definitions and symptom definitions in your custom policy settings.
- Apply the custom policy to object groups.

When you use an existing policy to create a custom policy, you override the policy settings to meet your own needs. You set the allocation and demand, the overcommit ratios for CPU and memory, and the thresholds for capacity risk and buffers. To allocate and configure what your environment is actually using, you use the allocation model and the demand model together. Depending on the type of environment you

monitor, such as a production environment versus a test or development environment, whether you over allocate at all and by how much depends on the workloads and environment to which the policy applies. You might be more conservative with the level of allocation in your test environment and less conservative in your production environment.

vRealize Operations Manager applies policies in priority order, as they appear on the Active Policies tab. When you establish the priority for your policies, vRealize Operations Manager applies the configured settings in the policies according to the policy rank order to analyze and report on your objects. To change the priority of a policy, you click and drag a policy row. The default policy is always kept at the bottom of the priority list, and the remaining list of active policies starts at priority 1, which indicates the highest priority policy. When you assign an object to be a member of multiple object groups, and you assign a different policy to each object group, vRealize Operations Manager associates the highest ranking policy with that object.

Your policies are unique to your environment. Because policies direct vRealize Operations Manager to monitor the objects in your environment, they are read-only and do not alter the state of your objects. For this reason, you can override the policy settings to fine-tune them until vRealize Operations Manager displays the results that are meaningful and that affect for your environment. For example, you can adjust the capacity buffer settings in your policy, and then view the data that appears in the dashboards to see the effect of the policy settings.

## **User Scenario: Create a Custom Operational Policy for a vSphere Production Environment**

As a system administrator of vRealize Operations Manager, you are responsible for ensuring that the objects in your vSphere environment conform to specific policies. You must ensure that your objects have enough memory and CPU to support your Test, Development, and Production environments.

Large IT environments might include four to six production environments that are organized according to object types, with a minor policy applied to each area. These large environments typically include a default policy, a single production policy that applies to the entire environment, and individual policies for dedicated areas.

You typically apply a default policy to most of the objects in your environment. To have vRealize Operations Manager monitor and analyze dedicated groups of objects, you create a separate policy for each object group, and make only minor changes in the settings for that policy. For example, you might apply a default operational policy for all of the objects in your vSphere production environment, but you also need to closely track the health and risk of virtual SQL Server instances, including their capacity levels. To have vRealize Operations Manager analyze only the virtual SQL Server instances, and to monitor them, you create a separate, dedicated policy and apply that policy to that group of objects. The settings in the policy that you create to monitor the virtual SQL Server instances differs only slightly from the main production policy.

This scenario shows you how to use multiple policies to analyze and monitor specific objects, so that you can manage them to ensure continuous operation. In this scenario, your vSphere production environment is one part of your overall production environment. You must create a custom operational policy to monitor the virtual SQL Server objects in your vSphere production environment.

## Prerequisites

- Understand the purpose of using a policy. See [Policies](#) .
- Verify that your vRealize Operations Manager instance is working properly.
- Verify that your vRealize Operations Manager instance includes the Default Policy and one or more other policies. See [Default Policy in vRealize Operations Manager](#).
- Understand the sections and elements in the policy, such as the attributes, alert and symptom definitions, and how the policy inherits settings from the base policies that you select. See [Policy Workspace in vRealize Operations Manager](#).
- Understand the analysis settings in the policy, such as capacity remaining and stress on hosts and virtual machines, and the actions used to override the settings inherited from the base policies. See the vRealize Operations Manager Information Center.

## Procedure

### 1 [Determine the vSphere Operational Requirements](#)

You must continuously monitor the capacity levels of your virtual SQL Server machines, and have vRealize Operations Manager notify you about any degradation in the performance of these objects. You want vRealize Operations Manager to notify you 60 days before these objects begin to experience problems with their capacity levels.

### 2 [Create a Policy to Meet vSphere Operational Needs](#)

You will create an operational policy for your virtual SQL Server instances, where only these settings differ from the main production policy. In this policy, you change the memory and CPU settings for specific objects. You then configure vRealize Operations Manager to send alerts to you when the performance degrades on your virtual SQL Servers.

### 3 [Configure the Custom Policy Settings to Analyze and Report on vSphere Objects](#)

You use different policy requirements for your Development, Test, and Production environments so that you can configure the specific policy settings for vRealize Operations Manager to analyze and report on your objects, including your virtual SQL Servers.

### 4 [Apply the Custom Policy to vSphere Object Groups](#)

You create an object group type to categorize your virtual SQL Server machines. Then you create an object group that contains your virtual SQL Server machines, and apply your custom policy to this group of SQL Server virtual machine objects.

## What to do next

After you finish this scenario, you must wait for vRealize Operations Manager to collect data from the objects in your environment. When a violation of the policy thresholds occur, vRealize Operations Manager sends an alert to notify you of the problem. If you continuously monitor the state of your objects, you are always aware of the state of the objects in your environment, and do not need to wait for vRealize Operations Manager to send alerts.

Create a custom dashboard so that you can monitor the virtual SQL Server objects and address problems that occur. See [Dashboards](#).

## Determine the vSphere Operational Requirements

You must continuously monitor the capacity levels of your virtual SQL Server machines, and have vRealize Operations Manager notify you about any degradation in the performance of these objects. You want vRealize Operations Manager to notify you 60 days before these objects begin to experience problems with their capacity levels.

Your VP of Infrastructure has defined a default operational policy and a main production policy for all of the objects in your production environment, and your IT Director has applied these policies to your production environments. Although the main production policy handles the operational monitoring needs for most of your objects, your manager requires that you be notified about any degradation in the performance of your production virtual SQL Server machines. You have vRealize Operations Manager continuously monitor the capacity levels of your virtual SQL Servers so that you can address problems that occur. You have vRealize Operations Manager notify you 60 days before your virtual SQL Servers begin to experience problems with their capacity levels.

Your IT department divided objects into dedicated groups that support the Development, Test, and Production areas. You must use vRealize Operations Manager to continually track and assess the health and risk of the objects in each of these areas.

In this scenario, you create an operational management policy to analyze, monitor, and troubleshoot your objects. You then monitor the results in custom dashboards.

You must first determine the vSphere operational requirements so that you can understand the analysis settings required for your policy. You can then create a policy to monitor your virtual SQL Server objects, and configure the custom policy to include minor differences in the settings for the main production policy.

When you create the custom policy to analyze and monitor your virtual SQL Servers, you configure the analysis settings so that vRealize Operations Manager analyzes specific objects and report the results in the dashboards. You then apply the policy to groups of virtual SQL Server objects.

### Prerequisites

Verify that the following conditions are met:

- You understand the context of this scenario. See [User Scenario: Create a Custom Operational Policy for a vSphere Production Environment](#).
- A default policy and a main production policy are in effect for all of the objects in your vSphere production environment.

### Procedure

- 1 Determine the operational requirements for your vSphere production environment.

In this scenario, the following requirements will be applied to the environment.

2 Develop a plan to create a custom operational policy that meets the requirements to analyze and monitor the objects in your environment.

- a Ensure that virtual SQL Servers continuously have adequate memory and CPU capacity.
- b Ensure that you do not overcommit memory on your production virtual SQL Servers.
- c Overcommit only a small percentage of the CPUs on your SQL Servers.

In this scenario, you set the value to 2. In some production environments, a typical value might be 4.

- d Ensure that vRealize Operations Manager alerts you if the capacity of your virtual SQL Servers drops below the defined thresholds.
- e Set the Co-Stop value on your production virtual SQL Servers to an acceptable level so that the SQL Servers do not experience delay because of CPU scheduling contention.
- f Determine whether to overcommit compute resources for certain ratios.

After you plan the custom policy requirements, you can implement the policy.

#### What to do next

Create an operational policy for your virtual SQL Server instances.

#### Create a Policy to Meet vSphere Operational Needs

You will create an operational policy for your virtual SQL Server instances, where only these settings differ from the main production policy. In this policy, you change the memory and CPU settings for specific objects. You then configure vRealize Operations Manager to send alerts to you when the performance degrades on your virtual SQL Servers.

In this procedure, you create a dedicated policy for a subset of virtual SQL Server objects, and change settings for the memory and CPU capacity for your virtual SQL Server instances. At this point in the scenario, your custom policy has only minor differences from the production policy.

The difference between the main production policy and your virtual SQL Server policy is in the overcommitment of compute resources. For the SQL Server policy, you do not overcommit compute resources. You have the SQL server policy inherit most of the settings from your overall production policy, except that you change the capacity settings that apply directly to the virtual SQL servers.

After you apply the main production policy to your entire production environment, you create the dedicated policy, have it inherit settings from the main policy, and make minor changes to settings in the dedicated policy to adjust the capacity levels for your virtual SQL Servers.

To create this policy, you choose a cluster that contains the data center and the vCenter Server that will use this policy. You make minor changes for all of the objects, including the cluster, data center, host system, resource pools, and the virtual machine resource containers.

## Prerequisites

Verify that the following conditions are met:

- You know the vSphere operational requirements. See [Determine the vSphere Operational Requirements](#).
- A default policy is in effect for your entire production environment of vSphere objects.

## Procedure

- 1 In vRealize Operations Manager, select **Administration > Policies**.

The **Active Policies** tab displays the current policies in effect.

- 2 Click the **Policy Library** tab, and click the plus sign to add a custom policy.
- 3 In the workspace navigation pane, click **Getting Started** and define the basic information for the policy.

- a In the **Name** text box, enter **vSphere Production Virtual SQL Servers**.
- b In the **Description** text box, enter **Analyze capacity of virtual SQL Servers**.
- c To start with a base policy, select **Default Policy** from the **Start with** drop-down menu.

- 4 View the policy configuration settings.

- a In the policy workspace, click **Select Base Policies**.
- b To view the policy configuration for virtual machine objects, click the **Show changes for** drop-down menu, click **vCenter Adapter - Virtual Machine**, and click the **Show object type** filter.  
The Virtual Machine policy configuration appears in the right pane.
- c To view the inherited settings, in the Policy Preview pane, click **Configuration inherited from base policy**.

- 5 In the workspace navigation, click **Analysis Settings**.

- 6 In the workspace navigation, add the following object types to the list so that you can change their settings.

- a Click the drop-down arrow, click **vCenter Adapter - Cluster Compute Resource**, and click the filter.
- b Click the drop-down arrow, click **vCenter Adapter - Data Center**, and click the filter.
- c Click the drop-down arrow, click **vCenter Adapter - Host System**, and click the filter.
- d Click the drop-down arrow, click **vCenter Adapter - Resource Pool**, and click the filter.
- e Click the drop-down arrow, click **vCenter Adapter - Virtual Machine**, and click the filter.

The analysis settings for these object types appear in the right pane.

- 7 On the Cluster Compute Resource bar, click the double arrows to expand the list of analysis settings.
- 8 Locate **Capacity Remaining Time Remaining** and click the lock button to enable changes.

- 9 In the resource table, set the overcommit for Memory Allocation value to **0** so that vRealize Operations Manager does not overcommit these objects for your SQL Server policy.
- 10 In the resource table, set the overcommit ratio for CPU Allocation to **2** so that vRealize Operations Manager overcommits a 2:1 ratio for CPU allocation on each SQL Server.
- 11 Repeat [Step 7](#) through [Step 10](#) for each object type that you added to the right pane.
- 12 Click **Save**.

You created a policy and made minor changes to settings so that vRealize Operations Manager can analyze and report on your SQL Server objects.

### What to do next

Configure the alert definitions and symptom definitions for your SQL Server policy. You will apply the policy to your SQL Server object groups.

### Configure the Custom Policy Settings to Analyze and Report on vSphere Objects

You use different policy requirements for your Development, Test, and Production environments so that you can configure the specific policy settings for vRealize Operations Manager to analyze and report on your objects, including your virtual SQL Servers.

This scenario presents several typical cases where you might be required to differentiate between the policy requirements for Development, Test, and Production environments.

- For your Development and Test environments, you might not be concerned if the objects in these environments experience network redundancy loss, but you do care when the objects fail. In this case, you locate the Physical NIC link state alert definition, double-click the state, and set it to Disabled.
- For a Test environment, you might not be concerned if your virtual machines demand more memory and CPU capacity than what is actually configured, because workloads can vary in test environments.
- For a Production environment, your virtual machines might require more memory than you have configured, which might cause a problem with the performance and reliability of your production environment.

In this procedure, you override the symptom definition threshold value for the Co-Stop performance of your virtual machines.

### Prerequisites

Verify that the following conditions are met:

- You created a custom policy for your virtual SQL Servers. See [Create a Policy to Meet vSphere Operational Needs](#).
- You understand the Co-Stop CPU performance metric for virtual machines. This metric represents the percentage of time that a virtual machine is ready to run, but experiences delay because of co-virtual CPU scheduling contention. Co-Stop is one of several performance metrics for virtual machines that also include Run, Wait, and Ready.

- The alert definition named Virtual machine has high CPU contention caused by Co-Stop, exists.
- Symptom definitions exist to track the critical, immediate, and warning levels of CPU Co-Stop on the virtual machines. For example, the critical level for virtual machine CPUs that experience contention more than 15% of the time is set to 15% by default, as measured by the Co-Stop metric. The default threshold level for Immediate is 10%, and for warning is 5%. However, in your production policy for your production virtual machines, you manage the critical level at 3%.

## Procedure

- 1 On the **Policy Library** tab, locate your vSphere Production Virtual SQL Servers policy, and click the pencil to edit the policy.

The Edit Monitoring Policy workspace appears.

- 2 In the workspace, click **Override Alert / Symptom Definitions**.
- 3 On the Alert Definitions pane, enable the Co-Stop alert definition to notify you about high CPU contention on your virtual machines.
  - a In the Object Type drop-down menu, select **vCenter Adapter** and **Virtual Machine**.
  - b In the **Search** text box, enter **stop** to display only the alert definitions that relate to the Co-Stop performance metric for virtual machines.
  - c For the Alert definition named Virtual machine has high CPU contention caused by Co-Stop, click the **State** drop-down menu and click **Enabled**.
- 4 In the Symptom Definitions pane, modify the critical Co-Stop level for virtual machines so that vRealize Operations Manager triggers an alert based on the threshold level defined for this symptom.
  - a In the Object Type drop-down menu, click **vCenter Adapter** and **Virtual Machine**.
  - b In the **Search** text box, enter **stop** to display the symptom definitions that apply to the Co-Stop performance metric for virtual machines.
  - c For the symptom definition named Virtual Machine CPU Co-stop is at Critical level, click the **State** drop-down menu and click **Enabled**.
  - d Click the **Condition** drop-down menu, and click **Override**.
 

For a production policy, a typical critical threshold value is >3. For a development or test environment policy, a typical critical threshold value is >10.
  - e In the Override Symptom Definition Threshold dialog box, enter >3 to change the threshold value, and click **Apply**.
- 5 Modify the immediate Co-Stop level for virtual machines.
  - a For the symptom definition named Virtual Machine CPU Co-stop is at Immediate level, click the **State** drop-down menu and click **Enabled**.
  - b Click the **Condition** drop-down menu, and click **Override**.
  - c In the Override Symptom Definition Threshold dialog box, enter >2 to change the threshold value, and click **Apply**.

- 6 Modify the warning Co-Stop level for virtual machines.
  - a For the symptom definition named `Virtual Machine CPU Co-stop is at Warning level`, click the **State** drop-down menu and click **Enabled**.
  - b Click the **Condition** drop-down menu, and click **Override**.
  - c In the Override Symptom Definition Threshold dialog box, enter **>1** to change the threshold value, and click **Apply**.
- 7 Click **Save** to save your policy.

You changed the Co-Stop CPU performance metric for virtual machines to minimize the delay on your SQL Server virtual machines because of CPU scheduling contention.

### What to do next

Create a group type to use to categorize your group of virtual SQL Servers, create an object group that contains your virtual SQL Servers, and apply the policy to your object group.

### Apply the Custom Policy to vSphere Object Groups

You create an object group type to categorize your virtual SQL Server machines. Then you create an object group that contains your virtual SQL Server machines, and apply your custom policy to this group of SQL Server virtual machine objects.

To have vRealize Operations Manager analyze your SQL Server machines according to the performance criteria in your custom policy, you must apply the custom policy to your group of SQL Server objects.

For this scenario, you create a static object group that contains your SQL Server virtual machines. In your own environment, you might need to create a dynamic object group so that vRealize Operations Manager discovers new SQL Server instances that become available to analyze and report on.

### Prerequisites

You configured the custom policy settings for your virtual SQL Server machines. See [Configure the Custom Policy Settings to Analyze and Report on vSphere Objects](#).

### Procedure

- 1 To create a group type for your virtual SQL Servers, click **Content** in the left pane, and click **Group Types**.
- 2 Click the plus sign to add a new object group type, and type **vSphere Production Virtual Machines**.  
You use this group type to categorize your SQL Server virtual machines for analysis.
- 3 Click **Environment** in the left pane, and click **Custom Groups**.  
A folder that corresponds to the group type that you just created appears in the list.
- 4 Click the folder named **vSphere Production Virtual Machines**, and click the plus sign to add a new object group.

- 5 In the New Group dialog box, add your SQL Server virtual machines.
  - a In the **Name** text box, type **vSphere Production SQL Server Virtual Machines**.
  - b From the **Group Type** drop-down menu, select **vSphere Production Virtual Machines**.
  - c From the **Policy** drop-down menu, select **vSphere Production Virtual SQL Servers**.
  - d In the object type drop-down menu in the Define Membership Criteria pane, expand **vCenter Adapter** and click **Virtual Machine**.
- 6 Click **OK** to save your object group.

After vRealize Operations Manager collects data, the **Groups** tab displays the status for the health, risk, and efficiency of the virtual machines in the object group.

You created an object type and object group to have vRealize Operations Manager analyze and report on the status of your SQL Server virtual machines.

### What to do next

Create a custom dashboard so that you can view the status of your virtual SQL Servers and address problems that occur. See [Dashboards](#).

Configure a modeling project that includes capacity planning scenarios for your production virtual SQL Servers to have vRealize Operations Manager monitor the capacity trends on these objects and notify you 60 days before your virtual SQL Servers experience capacity problems. See the vRealize Operations Manager Information Center.

Have vRealize Operations Manager report on the CPU use and memory use of your virtual machines on a regular schedule, and send the reports to you.

## Default Policy in vRealize Operations Manager

The default policy is a set of rules that applies to the majority of your objects.

The Default policy appears on the **Active Policies** tab, and is marked with the letter D in the Priority column. The Default policy can apply to any number of objects.

The Default policy always appears at the bottom in the list of policies, even if that policy is not associated with an object group. When an object group does not have a policy applied, vRealize Operations Manager associates the Default policy with that group.

A policy can inherit the Default policy settings, and those settings can apply to various objects under several conditions.

The policy that is set to Default always takes the lowest priority. If you attempt to set two policies as the Default policy, the first policy that you set to Default is initially set to the lowest priority. When you set the second policy to Default, that policy then takes the lowest priority, and the earlier policy that you set to Default is set to the second lowest priority.

You can use the Default policy as the base policy to create your own custom policy. You modify the default policy settings to create a policy that meets your analysis and monitoring needs. When you start with the Default policy, your new policy inherits all of the settings from the Default base policy. You can then customize your new policy and override these settings.

The data adapters and solutions installed in vRealize Operations Manager provide a collective group of base settings that apply to all objects. In the policy navigation tree on the **Policy Library** tab, these settings are called Base Settings. The Default policy inherits all of the base settings by default.

## Policies Provided with vRealize Operations Manager

vRealize Operations Manager includes sets of policies that you can use to monitor your environment, or as the starting point to create your own policies.

Verify that you are familiar with the policies provided with vRealize Operations Manager so that you can use them in your own environment, and to include settings in new policies that you create.

### Where You Find the Policies Provided with vRealize Operations Manager Policies

Click **Administration**, click **Policies**, click the **Policy Library** tab. To see the policies provided with vRealize Operations Manager, expand the Base Settings policy.

### Policies That vRealize Operations Manager Includes

All policies exist under the Base Settings, because the data adapters and solutions installed in your vRealize Operations Manager instance provide a collective group of base settings that apply to all objects. In the policy navigation tree on the **Policy Library** tab, these settings are called Base Settings.

The Base Settings policy is the umbrella policy for all other policies, and appears at the top of the policy list in the policy library. All of the other policies reside under the Base Settings, because the data adapters and solutions installed in your vRealize Operations Manager instance provide a collective group of base settings that apply to all objects.

The Config Wizard Based Policy set includes policies provided with vRealize Operations Manager that you use for specific settings on objects to report on your objects. The Config Wizard Based Policy set includes several types of policies:

- Capacity Management policies for Network I/O and Storage I/O
- Efficiency alerts policies for infrastructure objects and virtual machines
- Health alerts policies for infrastructure objects and virtual machines
- Overcommit policies for CPU and Memory
- Risk alerts policies for infrastructure objects and virtual machines

The Default Policy includes a set of rules that applies to the majority of your objects.

The VMware Management Policies set includes policies that you use for your type of environment, such as production as opposed to test and development. These policies contain settings that monitor for peak periods, batch and interactive workloads, and demand and allocation models. The VMware Management Policies set provided with vRealize Operations Manager include the following policies:

**Table 3-5. Functions of VMware Management Policies**

VMware Management Policy	What it does
VMware Excludes over-sized analysis	Does not calculate reclaimable capacity from oversized virtual machines
VMware Optimized for 15-minute peak periods	Configured to cause capacity alerts for workloads that spike for 15 minutes.
VMware Optimized for 30-minute peak periods	Configured to cause capacity alerts for workloads that spike for 30 minutes.
VMware Policy for Batch workloads	Optimized for batch workloads that run less than four hours.
VMware Policy for Interactive workloads	Configured to be sensitive toward interactive workloads, such as a desktop or Web server, based on 15-minute peaks with large buffers.
VMware Production Policy (Demand only)	Optimized for production loads, without using allocation limits, to obtain the most capacity.
VMware Production Policy (with Allocation)	Optimized for production loads that require the demand and allocation capacity models.
VMware Production Policy (without Allocation)	Optimized for production loads that require demand capacity models, and provides the highest overcommit without contention.
VMware Test and Dev Policy (without Allocation).	Optimized for Dev and Test environments to maximize capacity without causing significant contention, because it does not include capacity planning at the virtual machine level.

## Using the Monitoring Policy Workspace to Create and Modify Operational Policies

You can use the workflow in the monitoring policy workspace to create local policies quickly, and update the settings in existing policies. Select a base policy to use as the source for your local policy settings, and modify the thresholds and settings used for analysis and collection of data from groups of objects in your environment. A policy that has no local settings defined inherits the settings from its base policy to apply to the associated object groups.



Customize Operational Policies

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_customize\\_policies\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_customize_policies_vrom))

## Prerequisites

Verify that object groups exist for vRealize Operations Manager to analyze and collect data, and if they do not exist, create them. See [Managing Custom Object Groups in VMware vRealize Operations Manager](#).

## Procedure

- 1 Click **Administration**, and click **Policies**.
- 2 Click **Policy Library**, and click the plus sign to add a policy, or select the policy and click the pencil to edit an existing policy.

You can add and edit policies on the **Policy Library** tab, and remove certain policies. You can use the Base Settings policy or the Default Policy as the root policy for the settings in other policies that you create. You can set any policy to be the default policy.

- 3 In the Getting Started workspace, assign a name and description to the policy.  
Give the policy a meaningful name and description so that all users know the purpose of the policy.
- 4 Click **Select Base Policies**, and in the workspace, select one or more policies to use as a baseline to define the settings for your new local policy.

When you create a new policy, you can use any of the policies provided with vRealize Operations Manager as a baseline source for your new policy settings.

- 5 Click **Override Analysis Settings**, and in the workspace, filter the object types to customize your policy for the objects to associate with this policy.

Filter the object types, and modify the settings for those object types so that vRealize Operations Manager collects and displays the data that you expect in the dashboards and views.

- 6 Click **Override Attributes**, and in the workspace, select the metric, property, or super metric attributes to include in your policy.

vRealize Operations Manager collects data from the objects in your environment based on the metric, property, or super metric attributes that you include in the policy.

- 7 Click **Override Alert / Symptom Definitions**, and in the workspace, enable or disable the alert definitions and symptom definitions for your policy.

vRealize Operations Manager identifies problems on objects in your environment and triggers alerts when conditions occur that qualify as problems.

- 8 Click **Apply Policy to Groups**, and in the workspace, select one or more groups to which the policy applies.

VMware vRealize Operations Manager monitors the objects according to the settings in the policy that is applied to the object group, triggers alerts when thresholds are violated, and reports the results in the dashboards, views, and reports. If you do not assign a policy to one or more object groups, VMware vRealize Operations Manager does not assign the settings in that policy to any objects, and the policy is not active. For an object group that does not have a policy assigned, VMware vRealize Operations Manager associates the object group with the Default Policy.

9 Click **Save** to retain the settings defined for your local policy.

### What to do next

After vRealize Operations Manager analyzes and collects data from the objects in your environment, review the data in the dashboards and views. If the data is not what you expected, edit your local policy to customize and override the settings until the dashboards display the data that you need.

## Policy Workspace in vRealize Operations Manager

The policy workspace allows you to quickly create and modify policies. To create a new policy, you can inherit the settings from an existing policy, and you can modify the settings in existing policies if you have adequate permissions. After you create a new policy, or edit an existing policy, you can apply the policy to one or more groups of objects.

### How the Policy Workspace Works

Every policy includes a set of packages, and uses the defined problems, symptoms, metrics, and properties in those packages to apply to specific object groups in your environment. You can view details for the settings inherited from the base policy, and display specific settings for certain object types. You can override the settings of other policies, and include additional policy settings to apply to object types. For example, a critical production policy includes settings to track use, available resources and the time remaining on them, resource demands on the object group that determine how much stress is applied, and reclaimable capacity amounts for CPU, disk I/O, and network I/O.

Use the **Add** and **Edit** options to create new policies and edit existing policies.



Customize Operational Policies

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_customize\\_policies\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_customize_policies_vrom))

### Where You Create and Modify a Policy

To create and modify policies, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil icon to edit a policy. The policy workspace is where you select the base policies, and customize and override the settings for analysis, metrics, properties, alert definitions, and symptom definitions. In this workspace, you can apply the policy to object groups.

To remove a policy from the list, select the policy and click the red X.

### Policy Workspace Options

The policy workspace includes a step-by-step workflow to create and edit a policy, and apply the policy to custom object groups.

- [Getting Started Details](#)

When you create a policy, you must give the policy a meaningful name and description so that users know the purpose of the policy.

- [Select Base Policy Details](#)

You can use any of the policies provided with vRealize Operations Manager as a baseline source for your policy settings when you create a new policy. In the policy content area, you can view the packages and elements for the base policy and additional policies that you selected to override the settings, and compare the differences in settings highlighted between these policies. You select the settings and objects types to display.

- [Analysis Settings Details](#)

You can filter the object types, and modify the settings for those object types so that vRealize Operations Manager applies these settings. The data that you expect then appears in the dashboards and views.

- [Workload Automation Details](#)

You can set the workload automation options for your policy, so that vRealize Operations Manager can balance the workload in your environment per your definition.

- [Collect Metrics and Properties Details](#)

You can select the attribute type to include in your policy so that vRealize Operations Manager can collect data from the objects in your environment. Attribute types include metrics, properties, and super metrics. You enable or disable each metric, and determine whether to inherit the metrics from base policies that you selected in the workspace.

- [Alert and Symptom Definitions Details](#)

You can enable or disable alert and symptom definitions to have vRealize Operations Manager identify problems on objects in your environment and trigger alerts when conditions occur that qualify as problems. You can automate alerts.

- [Custom Profiles Details](#)

Custom profiles show how many more of a specified object can fit in your environment depending on the available capacity and object configuration. You can enable or disable custom profiles for your policy.

- [Apply Policy to Groups Details](#)

You can assign your local policy to one or more groups of objects to have VMware vRealize Operations Manager analyze those objects according to the settings in your policy, trigger alerts when the defined threshold levels are violated, and display the results in your dashboards, views, and reports.

## Getting Started Details

When you create a policy, you must give the policy a meaningful name and description so that users know the purpose of the policy.

### Where You Assign the Policy Name and Description

To add a name and description to a policy, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Getting Started**. The name and description appear in the workspace.

**Table 3-6. Name and Description Options in the Add or Edit Monitoring Policy Workspace**

Option	Description
Name	Name of the policy as it appears in the Add or Edit Monitoring Policy wizard, and in areas where the policy applies to objects, such as Custom Groups.
Description	Meaningful description of the policy. For example, use the description to indicate which policy is inherited, and any specific information that users need to understand the relationship of the policy to one or more groups of objects.
Start with	<p>The base policy that will be used as a starting point. All settings from the base policy will be inherited as default settings in your new policy. You can override these settings to customize the new policy.</p> <p>Select a base policy to inherit the base policy settings as a starting point for your new policy.</p>

## Select Base Policy Details

You can use any of the policies provided with vRealize Operations Manager as a baseline source for your policy settings when you create a new policy. In the policy content area, you can view the packages and elements for the base policy and additional policies that you selected to override the settings, and compare the differences in settings highlighted between these policies. You select the settings and objects types to display.

### How the Select Base Policies Workspace Works

To create a policy, select a base policy from which your new custom policy inherits settings. To override some of the settings in the base policy according to the requirements for the service level agreement for your environment, you can select and apply a separate policy for a management pack solution. The override policy includes specific settings defined for the types of objects to override, either manually or that an adapter provides when it is integrated with vRealize Operations Manager. The settings in the override policy overwrite the settings in the base policy that you selected.

When you select and apply a policy in the left pane to use to overwrite the settings that your policy inherits from the base policy, the policy that you select appears in the applied policy history list in the right pane.

The right pane displays tabs for the inherited policy configuration, and your policy, and displays a preview of the selected policy tab in the Policy Preview pane. When you select one of the policy tabs, you can view the number of enabled and disabled alert definitions, symptom definitions, metrics and properties, and the number of enabled and disabled changes.

In the right pane, you select the objects to view so that you can see which policy elements apply to the object type. For example, when you select the StorageArray object type, and you click the tab to display the configuration settings for your policy, the Policy Preview pane displays the local packages for the policy and the object group types with the number of policy elements in each group.

You can preview the policy settings for all object types, only the object types that have settings changed locally, or settings for new object types that you add to the list, such as Storage Array storage devices.

## Where You Select and Override Base Policies Settings

To select a base policy to use as a starting point for your own policy, and to select a policy to override one or more settings that your policy inherits from the base policy, select **Administration > Policies > Policy Library** and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left add a name for the policy and click **Select Base Policies**. The policy configuration, objects, and preview appear in the workspace.

**Table 3-7. Base Policy and Override Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Show changes for	<p>Select the objects to view changes.</p> <ul style="list-style-type: none"> <li>■ All object types. Displays the number of enabled and disabled alert definitions, symptom definitions, and metrics and properties, the number of enabled and disabled changes, and the object type groups and the number of local policy elements for each group.</li> <li>■ All object types with overrides. Displays the object types that have changes applied, with the objects types selected for override. Use the drop-down menu to select object types. Click the filter button to add the selected object type to the list so that you can preview and configure the settings.</li> <li>■ Add settings for new set of objects. Provides a list of the object types so that you can select an object type, such as <b>Storage Devices &gt; SAN</b>, and add the selected object to the Object types list.</li> </ul>
Override settings from additional policies	Select and apply one or more policies to override the settings that your policy inherits from the base policy.
Apply	Applies the override policy to your policy, and lists the override policy in the applied policy history.
Applied policy history	Displays the policies that you selected to override the settings in your policy.
Configuration inherited from base policy	When selected, displays a preview of the inherited policy configuration in the Policy Preview pane.
Configuration settings defined in this policy	When selected, displays a preview of your policy configuration in the Policy Preview pane.
Policy Preview	<p>Displays summary information about the local packages and object group types.</p> <ul style="list-style-type: none"> <li>■ Packages (Local). Displays the number of enabled and disabled alert definitions, symptom definitions, metrics and properties, and the number of policy elements for each object group.</li> <li>■ Object Type groups. Displays the associated object groups.</li> <li>■ Drop down arrows on packages and settings. Displays the packages and settings for the displayed policies.</li> </ul>

## Analysis Settings Details

You can filter the object types, and modify the settings for those object types so that vRealize Operations Manager applies these settings. The data that you expect then appears in the dashboards and views.

## How the Analysis Settings Workspace Works

When you turn on and configure the analysis settings for a policy, you can override the settings for the policy elements that vRealize Operations Manager uses to trigger alerts and display data. These types of settings include badge score symptom thresholds based on alerts, situational settings such as committed projects to calculate capacity and time remaining, and other detailed settings.

You expand a policy element setting and configure the values to make your policy specific. For example, to reclaim capacity, you can set percentages to have vRealize Operations Manager indicate when a resource is oversized, idle, or powered off.

Policies focus on objects and object groups. When you configure policy element settings for your local policy, you must consider the object type and the results that you expect to see in the dashboards and views. If you do not make any changes to the settings, your local policy retains the settings that your policy inherited from the base policy that you selected.

## Where You Set the Policy Analysis Settings

To set the analysis settings for your policy, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Analysis Settings**. The analysis settings for host systems, virtual machines, and other object types that you select appear in the workspace.

**Table 3-8. Analysis Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Show changes for	<p>Select the objects to view changes.</p> <ul style="list-style-type: none"> <li>■ All object types. Displays the number of enabled and disabled alert definitions, symptom definitions, and metrics and properties, the number of enabled and disabled changes, and the object type groups and the number of local policy elements for each group.</li> <li>■ All object types with overrides. Displays the object types that have changes applied, with the objects types selected for override. Use the drop-down menu to select object types. Click the filter button to add the selected object type to the list so that you can preview and configure the settings.</li> <li>■ Add settings for new set of objects. Provides a list of the object types so that you can select an object type, such as <b>Storage Devices &gt; SAN</b>, and add the selected object to the Object types list.</li> </ul>
Right pane - Analysis Settings for object types	<p>The right pane displays a list of the object types that you selected in the left pane.</p> <p>Expand a view of the policy elements and settings for the object type so that you can have vRealize Operations Manager analyze the object type.</p> <p>Expand the view for the object type so that you can view and modify the threshold settings for the following policy elements:</p> <ul style="list-style-type: none"> <li>■ Workload</li> <li>■ Anomaly</li> <li>■ Fault</li> <li>■ Capacity and Time Remaining</li> <li>■ Stress</li> <li>■ Compliance</li> <li>■ Reclaimable Capacity</li> <li>■ Density</li> <li>■ Time Range</li> </ul> <p>Click the lock icon on the right of each element to override the settings and change the thresholds for your policy.</p>

### Policy Workload Element

Workload is a measurement of the demand for resources on an object. You can turn on and configure the settings for the Workload element for the object types in your policy. You can then override the settings and have vRealize Operations Manager calculate the metrics for CPU use and memory use, and display the demand for resources on the selected objects, based on your settings.

#### How the Workload Element Works

The Workload element determines how vRealize Operations Manager reports on the resources that the selected object group uses. The resources available to the object group depend on the amount of configured and usable resources.

- A specific amount of physical memory is a configured resource for a host system, and a specific number of CPUs is a configured resource for a virtual machine.
- The usable resource for an object or an object group is a subset of, or equal to, the configured amount.

- The configured and usable amount of a resource can vary depending on the type of resource and the amount of virtualization overhead required, such as the memory that an ESX host machine requires to run the host system. When accounting for overhead, the resources required for overhead are not considered to be usable, because of the reservations required for virtual machines or for the high availability buffer.

### Where You Override the Policy Workload Element

To view and override the policy Workload analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The workload settings for the object types that you selected appear in the right pane.

View the Workload policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-9. Policy Workload Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Workload drop-down menu	When expanded, displays a list of the resource containers. You can enable or disable the resource containers for the workload calculation.
Badge Score Symptom Threshold	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Workload</b> to view the badge score symptom thresholds for Workload policy settings for a selected object, as defined in the policy applied to the object.</p>

**Table 3-10. Policy Workload Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Workload drop-down menu	When expanded, displays a list of the resource containers. You can enable or disable the resource containers for the workload calculation.
Badge Score Symptom Threshold	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Workload</b> to view the badge score symptom thresholds for Workload policy settings for a selected object, as defined in the policy applied to the object.</p>

## Policy Anomaly Element

An anomaly is an unusual or abnormal event that occurs on an object. You can turn on and configure the settings for the Anomaly element for the object types in your policy so that you can override the settings and have vRealize Operations Manager determine the acceptable level of abnormal behavior for an object according to the historical metrics data for that object, based on your settings.

### Where You Override the Policy Anomaly Element

To view and override the policy Anomaly analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The anomalies settings for the object types that you selected appear in the right pane.

View the Anomaly policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-11. Policy Anomaly Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Badge Score Symptom Threshold	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Anomalies</b> to view the badge score symptom thresholds for Anomalies policy settings, as defined in the policy applied to the object.</p>

## Policy Fault Element

A fault is an object-based error condition, such as Guest file system out of space for a virtual machine, or Host connectivity for a host system. You can turn on and configure the settings for the Fault element for the object types in your policy so that you can override the settings and have vRealize Operations Manager determine and quantify the severity of problems experienced by selected objects, based on your settings.

### Where You Override the Policy Fault Element

To view and override the policy Fault analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The fault settings for the object types that you selected appear in the right pane.

View the Fault policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-12. Policy Fault Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Overrides button	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Badge Score Symptom Threshold	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Faults</b> to view the badge score symptom thresholds for Faults policy settings for a selected object, as defined in the policy applied to the object.</p>

### Policy Capacity Remaining and Time Remaining Element

Capacity is a measurement of the amount of memory, CPU, and disk space for an object. Time remaining is a measure of the amount of time left before your objects run out of capacity. You can turn on and configure the settings for the Capacity Remaining and Time Remaining element for the object types in your policy so that you can override the settings and have vRealize Operations Manager report on the available capacity remaining and the amount of time remaining before resources run out, based on your settings.

#### How the Capacity Remaining and Time Remaining Element Works

The Capacity Remaining and Time Remaining element determines how vRealize Operations Manager reports on the available capacity and time until resources run out for a specific object type group.

- The capacity remaining indicates the capability of your environment to accommodate new machines. vRealize Operations Manager calculates the capacity remaining as a percentage of the overall capacity that remains for the number of virtual machines, compared to the total number of virtual machines that can be deployed on the selected object.
- The time remaining indicates the amount of time that remains before the object group consumes all of the resources. vRealize Operations Manager calculates the time remaining as the number of days remaining until all of the capacity would be consumed, minus the number of days allocated to the provisioning buffer.
- Usable capacity is a measurement of the percentage of capacity available, minus the capacity affected when you use high availability, and you set capacity buffer amounts on the memory, CPU, network, datastore, and disk space buffers. If you set overcommit values, the usable capacity measurement adds the capacity to the amount of usable capacity available.
- You can modify the usable capacity settings to use high availability so that vRealize Operations Manager provides enough objects and resources to address throughput and any potential loss of data. You can also modify the calculation type and the buffer rules.

- Capacity settings for resource containers are enabled or disabled for analysis. For the Memory, CPU, and Disk Space resource containers, you can enable or disable the demand and allocation. For the Network I/O resource container, you can enable or disable the data transmit rate, data receive rate, and the use rate. For the Datastore I/O resource container, you can enable or disable the outstanding I/O requests, reads and writes per second, and the read and write rate. You can also enable or disable the vSphere configuration limit.
- The peak consideration setting causes vRealize Operations Manager to apply stress settings to account for peak uses in capacity.
- You can have vRealize Operations Manager account for committed projects that you defined so that you can plan the future capacity of your objects. Because committed projects are scenarios that forecast the future capacity of objects, accounting for committed projects affects the time remaining score.
- The number of days set for the provisioning time buffer is based on the amount of time you require to provision the objects in your environment, from the time of ordering those objects to deploying them. To keep the Time Remaining score above zero, your objects must have more days of capacity available than the provisioning time buffer.

### Where You Override the Policy Capacity Remaining and Time Remaining Element

To view and override the policy Capacity Remaining and Time Remaining analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The capacity remaining and time remaining settings for the object types that you selected in the workspace appear in the right pane.

View the Capacity Remaining and Time Remaining policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-13. Policy Capacity Remaining and Time Remaining Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Symptom Thresholds for Time Remaining Score and Capacity Score	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>The badge score symptom threshold for the Capacity Remaining and Time Remaining policy settings appear on the following tabs for a selected object:</p> <ul style="list-style-type: none"> <li>■ <b>Environment &gt; Object &gt; Analysis &gt; Capacity Remaining</b></li> <li>■ <b>Environment &gt; Object &gt; Analysis &gt; Time Remaining</b></li> </ul>

Option	Description
Usable Capacity settings for resource containers	<p>Displays the selected resource containers and resources to include in the analysis, overcommit types and values for resources such as memory and CPU, and the capacity buffer percentage for each resource container.</p> <ul style="list-style-type: none"> <li>■ Capacity Buffer %. Defines the percentage of capacity reserved on virtual machines so that the virtual machine does not consume all of its resources. The capacity buffers are defined on Cluster objects and Host objects to reserve some resources for failover.</li> <li>■ Overcommit. Displays the over commitment type, such as memory or CPU.</li> <li>■ Value. Displays the amount of over commitment on capacity resources.</li> </ul> <p>To change these settings, select a resource container and double-click the value you want to change.</p>
Additional settings that affect time and capacity remaining calculations	<p>The available settings depend on the object type you select.</p> <ul style="list-style-type: none"> <li>■</li> <li>■ High Availability. When selected, vRealize Operations Manager report on the capacity available to the object type group.</li> </ul> <p>You can have vRealize Operations Manager take into consideration the High Availability (HA) settings.</p> <ul style="list-style-type: none"> <li>■ Peak Consideration. When selected, vRealize Operations Manager includes the Stress element in the capacity remaining and time remaining calculations.</li> <li>■ Committed Projects. When selected, if you committed one or more projects on an object type, and added capacity scenarios to those projects to plan for future capacity requirements, vRealize Operations Manager accounts for the committed projects in the capacity remaining and time remaining calculations.</li> <li>■ Capacity Calculation. Indicates on what status vRealize Operations Manager reports. You can select either the current value or a trend of values as the basis for the capacity analysis.</li> <li>■ Provisioning Time Buffer. Indicates the number of days allowed to provision physical or virtual resources. vRealize Operations Manager uses this number to calculate the capacity remaining and time remaining for resource types, and shortens the time remaining scores.</li> </ul> <p>Peak consideration, committed projects, and the provisioning buffer settings, as defined in the applied policy, appear on the following tabs for a selected object.</p> <ul style="list-style-type: none"> <li>■ <b>Environment &gt; Object &gt; Analysis &gt; Capacity Remaining</b></li> <li>■ <b>Environment &gt; Object &gt; Analysis &gt; Time Remaining</b></li> </ul>

## Policy Stress Element

Stress is a measurement of the workload on an object over time, including CPU, memory, network I/O, and datastore I/O. You can turn on and configure the settings for the Stress element for the object types in your policy so that you can override the settings and have vRealize Operations Manager analyze the resources used for an object or object group over a period of time, and report the historical workload based on your settings.

### How the Stress Element Works

The Stress element determines how vRealize Operations Manager reports on the demand for resources and usable capacity over time.

- When you include the Stress element in your policy, you can use the stress score to identify hosts and machines that require additional resources, and identify hosts that require fewer virtual machines, so that you can avoid performance problems in your environment.

- When you select Peak Consideration in the Capacity & Time Remaining element, vRealize Operations Manager can use the Stress element to account for peaks in capacity usage.
- Stress is the percentage of demand over time, where stress extends above the stress noise line. For example, the stress line might be 70 percent of the percentage of workload over time, based on the setting used for exceeding the demand. As vRealize Operations Manager calculates capacity and time remaining, you might want to account for these spikes and peaks.

To set the stress settings, use the sliding analysis settings. The settings for stress might need to differ between policies used to monitor your infrastructure versus virtual machines. For example, for an infrastructure policy, your recommended levels for the stress settings might be 10 (warning), 30 (immediate), and 50 (critical). For virtual machines, the settings might be 5 (warning), 10 (immediate), and 20 (critical). For a test and development policy, you might want vRealize Operations Manager to trigger an alert when the level reaches 10 percent. For a production policy, you typically want to ensure that sufficient capacity exists for peak use.

### Where You Override the Policy Stress Element

To view and override the policy Stress analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The stress settings for the object types that you selected appear in the right pane.

View the Stress policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-14. Policy Stress Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Symptom Thresholds for Time Remaining Score and Capacity Score	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Stress</b> to view the badge score symptom thresholds for Stress policy settings for a selected object, as defined in the policy applied to the object.</p>
Stress settings for resource containers	<p>Displays the resource container and settings for exceeding the demand during the time range defined in the policy Time element.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Stress</b> to view the percentage for exceeding demand for a selected object, as defined in the applied policy.</p> <p>The Sliding Analysis Window defines the time period that vRealize Operations Manager checks for stress, which occurs at the defined range of minutes, or during the entire range defined for the data range in the Time policy element, to monitor for peak stress periods. To modify the setting, select the resource container setting, such as <b>Disk Space &gt; Usage</b>, double-click the Sliding Analysis Window setting, and select either <b>Any</b> or <b>Entire Range</b>. When the setting is Any, you can modify the Minute Peak value to an interval in minutes for vRealize Operations Manager to monitor your objects and report on peak times of stress.</p>

## Policy Compliance Element

Compliance is a measurement that ensures that the objects in your environment meet industrial, governmental, regulatory, or internal standards. You can unlock and configure the settings for the Compliance element for the object types in your policy. You can override the base policy settings and have vRealize Operations Manager report on the compliance results for virtual machines and related objects, such as the ratios of virtual machines to hosts, memory demand, and CPU demand.

### Where You Override the Policy Compliance Element

To view and override the policy Compliance analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The compliance settings for the object types that you selected appear in the right pane.

View the Compliance policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-15. Policy Compliance Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Badge Score Symptom Threshold	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Compliance</b> to view the badge score symptom thresholds for Compliance policy settings for a selected object, as defined in the policy applied to the object.</p>

## Policy Reclaimable Capacity Element

Reclaimable capacity is a measurement of the CPU, memory, and disk space for your objects that is designated as waste. You can turn on and configure the settings for the Reclaimable Capacity element for the object types in your policy so that you can override the settings and have vRealize Operations Manager analyze and report on the capacity that you can reclaim from unused or underused objects. You can then provision the reclaimed capacity to other objects in your environment, based on your settings.

### How the Reclaimable Capacity Element Works

The Reclaimable Capacity element determines how vRealize Operations Manager reports the amount of reclaimable capacity of objects such as CPU, memory, and disk space for each object in your environment.

When you include the reclaimable capacity element in your policy, you can use the reclaimable capacity score to identify the amount of resources that can be reclaimed and provisioned to other objects.

## Where You Override the Policy Reclaimable Capacity Element

To view and override the policy Reclaimable Capacity analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The reclaimable capacity settings for the object types that you selected appear in the right pane.

View the Reclaimable Capacity policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-16. Policy Reclaimable Capacity Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Badge Score Symptom Threshold	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Reclaimable Capacity</b> to view the badge score symptom thresholds for Reclaimable Capacity policy settings for a selected object, as defined in the policy applied to the object.</p>
Reclaimable capacity settings for resource containers	<p>Displays the configurable percentages for vRealize Operations Manager to use to report when a resource is determined to be oversized, idle, or powered off.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Reclaimable Capacity</b> to view the settings for disk and CPU idle levels, and the percentages used to determine when a resource is oversized, idle, or powered off for a selected object, as defined in the policy applied to the object.</p> <p>For the selected object, you can set the Oversized, Idle, and Powered Off, and Unused capacity settings.</p> <ul style="list-style-type: none"> <li>■ An object is considered to be oversized when its recommended capacity is less than the defined percentage of its current capacity. For example, when the Oversized setting for a virtual machine is 50%, the virtual machine is considered to be oversized when its capacity is half of the current capacity available.</li> <li>■ An object is considered to be idle when the object operates below the idle level for the defined percentage of time. For example, when the CPU idle level is set to 100 MHz for a virtual machine, and the flag for the idle level is set to 90%, the virtual machine is considered to be idle when the speed of its CPU drops below 100 MHz for 90% of the time.</li> <li>■ An object is flagged as powered off when the object is powered down for the defined percentage of time. For example, when the powered off flag is set to 90%, a virtual machine is flagged as powered off when it is powered down at least 90% of the time.</li> <li>■ An object is considered to be unused when its timestamp attribute has not changed for the defined number of days, which means that the object has not been accessed. For example, when the flag for the disk space reclaimable snapshot space is set to 60 days for a virtual machine, if the virtual machine or the files on it have not been accessed for 60 days, the virtual machine is considered to be unused.</li> </ul>

## Policy Density Element

Density is a measurement of the sizing ratio of your objects based on available CPU as opposed to demand, and available memory as opposed to demand. You can unlock and configure the settings for the Density element for the object types in your policy. You can override the base policy settings and have vRealize Operations Manager report on the density results for virtual machines and related objects, such as the ratios of virtual machines to hosts, memory demand, and CPU demand. For example, to reduce the virtual machine density on a host machine, move some of the virtual machines to another host.

### Where You Override the Policy Density Element

To view and override the policy Density analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The density settings for the object types that you selected appear in the right pane.

View the Density policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-17. Policy Density Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Badge Score Symptom Threshold	<p>Set the symptom threshold values for the policy element to levels that update the badge scores to meet the criteria for your environment. vRealize Operations Manager uses the symptom threshold values to trigger alerts that appear in the Alerts Overview and Dashboard scores.</p> <p>Select <b>Environment &gt; Object &gt; Analysis &gt; Density</b> to view the badge score symptom thresholds for Density policy settings for a selected object, as defined in the policy applied to the object.</p>

## Policy Time Element

Time indicates the schedule and range of days and hours that vRealize Operations Manager monitors the use of resources for your objects, and the maintenance schedule selected for periodic and repeatable maintenance. You can turn on and configure the settings for the Time element for the object types in your policy so that you can override the settings and have vRealize Operations Manager report on metrics and calculate analytics for the group at specific times.

### How the Time Element Works

The Time element determines when and how vRealize Operations Manager tracks resources on a specific object type.

### Where You Override the Policy Time Element

To view and override the policy Time analysis setting, click **Administration**, click **Policies**, and click the **Policy Library** tab. Click the plus sign to create a policy or the pencil to edit a selected policy. In the Add or Edit Monitoring policy workspace, click **Analysis Settings**, then select one or more objects in the left pane. The time settings for the object types that you selected appear in the right pane.

View the Time policy element, and configure the settings for your policy.

If you do not configure the policy element, your policy inherits the settings from the selected base policy.

**Table 3-18. Policy Time Element Settings in the Add or Edit Monitoring Policy Workspace**

Option	Description
Lock icon	Enables you to override the policy element settings so that you can customize the policy to monitor the objects in your environment.
Track Usage	Determines the times when vRealize Operations Manager runs the capacity analytics calculations. <ul style="list-style-type: none"> <li>■ At all times. Monitor the amount of time tracked 24 hours a day, 7 days a week.</li> <li>■ Specific days and times. Select when to track the time use.</li> </ul>
Data Range	Sets the number of days to include in the analysis of time use.
Maintenance Schedule	Sets a time to perform maintenance tasks. During maintenance times, vRealize Operations Manager does not calculate analytics.

## Workload Automation Details

You can set the workload automation options for your policy, so that vRealize Operations Manager can balance the workload in your environment per your definition.

### How the Workload Automation Workspace Works

You click the lock icon to unlock and configure the workload automation options specific for your policy. When you click the lock icon to lock the option your policy inherits the parent policy settings. The graphic on the right updates to reflect your changes.

### Where You Set the Policy Workload Automation

To set the workload automation for your policy, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Workload Automation**.

**Table 3-19. Workload Automation in the Add or Edit Monitoring Policy Workspace**

Option	Description
Balance Workloads	Select how vRealize Operations Manager balances the workload. Select Aggressive balancing when you have stable populations. It minimizes contention but moves workloads more, which can cause disruption. Select Conservative balancing when you have dynamic populations. It exposes potential contention, but moves workloads less.
Consolidate Workloads	Select how vRealize Operations Manager combines the workload. The consolidation policy setting does not affect the placement of virtual machines across clusters. <ul style="list-style-type: none"> <li>■ Select more consolidation when you have populations with steady demand. It puts workloads into as few hosts as possible to reduce licensing and power costs. However, this approach might cause less responsive capacity.</li> <li>■ Select less consolidation when you have population with irregular demand. It uses all available hosts, which leaves more room for demand spikes. However, this approach increases licensing and power costs.</li> </ul>
Advanced Settings	Click <b>Advanced Settings</b> to select what type of virtual machines vRealize Operations Manager moves first to address workload.

## Collect Metrics and Properties Details

You can select the attribute type to include in your policy so that vRealize Operations Manager can collect data from the objects in your environment. Attribute types include metrics, properties, and super metrics. You enable or disable each metric, and determine whether to inherit the metrics from base policies that you selected in the workspace.

### How the Collect Metrics and Properties Workspace Works

When you create or customize a policy, you can override the base policy settings to have vRealize Operations Manager collect the data that you intend to use to generate alerts, and report the results in the dashboard scores.



Editing Metrics Collected in vRealize Operations Manager Using a Policy  
([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_editing\\_metrics\\_with\\_policy\\_in\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_editing_metrics_with_policy_in_vrom))

You define the metric and super metric symptoms, metric event symptoms, and property symptoms in **Content > Symptom Definitions**.

### Where You Override the Policy Attributes

To override the attributes and properties settings for your policy, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil icon to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Collect Metrics and Properties**. The attributes and properties settings for the selected object types appear in the workspace.

**Table 3-20. Collect Metrics and Properties Options**

Option	Description
Actions	Select one or more attributes and select enable, disable, or inherit to change the state and KPI for this policy.
Filter options	<p>Deselect the options in the <b>Attribute Type</b>, <b>State</b>, <b>KPI</b>, and <b>DT</b> drop-down menus, to narrow the list of attributes.</p> <ul style="list-style-type: none"> <li>■  Enabled. Indicates that an attribute will be calculated.</li> <li>■  Enabled (Force). Indicates state change due to a dependency.</li> <li>■  Disabled. Indicates that an attribute will not be calculated.</li> <li>■  Inherited. Indicates that the state of this attribute is inherited from the base policy and will be calculated.</li> <li>■  Inherited. Indicates that the state of this attribute is inherited from the base policy and will not be calculated.</li> </ul> <p>The KPI determines whether the metric, property, or super metric attribute is considered to be a key performance indicator (KPI) when vRealize Operations Manager reports the collected data in the dashboards. Filter the KPI states to display attributes with KPI enabled, disabled, or inherited for the policy.</p>
Object Type	Filters the attributes list by object type.
Page Size	The number of attributes to list per page.
Attributes data grid	<p>Display the attributes for a specific object type.</p> <ul style="list-style-type: none"> <li>■ Name. Identifies the name of the metric or property for the selected object type.</li> <li>■ Type. Distinguishes the type of attribute to be either a metric, property, or super metric.</li> <li>■ Adapter Type. Identifies the adapter used based on the object type selected, such as Storage Devices.</li> <li>■ Object Type. Identifies the type of object in your environment, such as StorageArray.</li> <li>■ State. Indicates whether the metric, property, or super metric is inherited from the base policy.</li> <li>■ KPI. Indicates whether the key performance indicator is inherited from the base policy. If a violation against a KPI occurs, vRealize Operations Manager generates an alert.</li> <li>■ DT. Indicates whether the dynamic threshold (DT) is inherited from the base policy.</li> </ul>

## Alert and Symptom Definitions Details

You can enable or disable alert and symptom definitions to have vRealize Operations Manager identify problems on objects in your environment and trigger alerts when conditions occur that qualify as problems. You can automate alerts.

### How the Alert and Symptom Definitions Workspace Works

vRealize Operations Manager collects data for objects and compares the collected data to the alert definitions and symptom definitions defined for that object type. Alert definitions include associated symptom definitions, which identify conditions on attributes, properties, metrics, and events.

You can configure your local policy to inherit alert definitions from the base policies that you select, or you can override the alert definitions and symptom definitions for your local policy.

Before you add or override the alert definitions and symptom definitions for a policy, familiarize yourself on the available alerts and symptoms.

- To view the available alert definitions, select **Content** and click **Alert Definitions**.
- To view the available symptom definitions, select **Content** and click **Symptom Definitions**. Symptom definitions are available for metrics, properties, messages, faults, smart early warnings, and external events.

A summary of the number of problem and symptoms that are enabled and disabled, and the difference in changes of the problem and symptoms as compared to the base policy, appear in the Analysis Settings pane of the policies workspace.

### Where You Override the Alert Definitions and Symptom Definitions

To override the alert definitions and symptom definitions for your policy, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Alert / Symptom Definitions**. The definitions appear in the workspace.

### Policy Alert Definitions and Symptom Definitions

You can override the alert definitions and symptom definitions for each policy.

- [Policy Alert Definitions](#)

Each policy includes alert definitions. Each alert uses a combination of symptoms and recommendations to identify a condition that classifies as a problem, such as failures or high stress. You can enable or disable the alert definitions in your policy, and you can set actions to be automated when an alert triggers.

- [Policy Symptom Definitions](#)

Each policy includes a package of symptom definitions. Each symptom represents a distinct test condition on a property, metric, or event. You can enable or disable the symptom definitions in your policy.

### Policy Alert Definitions

Each policy includes alert definitions. Each alert uses a combination of symptoms and recommendations to identify a condition that classifies as a problem, such as failures or high stress. You can enable or disable the alert definitions in your policy, and you can set actions to be automated when an alert triggers.

### How the Policy Alert Definitions Work

vRealize Operations Manager uses problems to trigger alerts. A problem manifests when a set of symptoms exists for an object, and requires you to take action on the problem. Alerts indicate problems in your environment. vRealize Operations Manager generates alerts when the collected data for an object is compared to alert definitions for that object type and the defined symptoms are true. When an alert occurs, vRealize Operations Manager presents the triggering symptoms for you to take action.

Some of the alert definitions include predefined symptoms. When you include symptoms in an alert definition, and enable the alert, an alert is generated when the symptoms are true.

The Alert Definitions pane displays the name of the alert, the number of symptoms defined, the adapter, object types such as host or cluster, and whether the alert is enabled as indicated by **Local**, disabled as indicated by **not Local**, or inherited. Alerts are inherited with a green checkmark by default, which means that they are enabled.

You can automate an alert definition in a policy when the highest priority recommendation for the alert has an associated action.

To view a specific set of alerts, you can select the badge type, criticality type, and the state of the alert to filter the view. For example, you can set the policy to send fault alerts for virtual machines.

### Where You Modify the Policy Alert Definitions

To modify the alerts associated with policies, click **Administration** in the left pane, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Alert / Symptom Definitions**. The alert definitions and symptom definitions for the selected object types appear in the workspace.

**Table 3-21. Alert Definitions in the Add or Edit Monitoring Policy Workspace**

Option	Description
Actions	Select one or more alert definitions and select enable, disable, or inherit to change the state for this policy.
Filter options	<p>Deselect the options in the <b>Type</b> and <b>State</b> drop-down menus, to narrow the list of symptom definitions.</p> <p>Impact indicates the health, risk, and efficiency badges to which the alerts apply.</p> <p>Criticality indicates the information, critical, immediate, warning, or automatic criticality types to which the alert definition applies.</p> <p>Automate indicates the actions that are enabled for automation when an alert triggers, or actions that are disabled or inherited. Actions that are enabled for automation might appear as inherited with a green checkmark, because policies can inherit settings from each other. For example, if the Automate setting in the base policy is set to <b>Local</b> with a green checkmark, other policies that inherit this setting will display the setting as inherited with a green checkmark.</p>
Object Type	Filters the alert definitions list by object type.
Page Size	The number of alert definitions to list per page.

Option	Description
Filter	Locates data in the alert definition list.
Alert Definitions data grid	<p data-bbox="518 262 1426 367">Displays information about the alert definitions for the object types. The full name for Alert definition and the criticality icon appear in a tooltip when you hover the mouse over the Alert Definition name.</p> <ul style="list-style-type: none"> <li data-bbox="518 367 1426 409">■ Name. Meaningful name for the alert definition.</li> <li data-bbox="518 409 1426 451">■ Symptom Definitions. Number of symptoms defined for the alert.</li> <li data-bbox="518 451 1426 514">■ Actionable Recommendations. Only recommendations with actions in the first priority, as they are the only ones you can automate.</li> <li data-bbox="518 514 1426 682">■ Automate. When the action is set to Local, the action is enabled for automation when an alert triggers. Actions that are enabled for automation might appear as inherited with a green checkmark, because policies can inherit settings from each other. For example, if the Automate setting in the base policy is set to <b>Local</b> with a green checkmark, other policies that inherit this setting will display the setting as inherited with a green checkmark.</li> <li data-bbox="518 682 1426 724">■ Adapter. Data source type for which the alert is defined.</li> <li data-bbox="518 724 1426 766">■ Object Type. Type of object to which the alert applies.</li> <li data-bbox="518 766 1426 823">■ State. Alert definition state, either enabled as indicated by <b>Local</b>, disabled as indicated by <b>not Local</b>, or inherited from the base policy.</li> </ul>

If you do not configure the package, the policy inherits the settings from the selected base policy.

## Policy Symptom Definitions

Each policy includes a package of symptom definitions. Each symptom represents a distinct test condition on a property, metric, or event. You can enable or disable the symptom definitions in your policy.

### How the Policy Symptom Definitions Work

vRealize Operations Manager uses symptoms that are enabled to generate alerts. When the symptoms used in an alert definition are true, and the alert is enabled, an alert is generated.

When a symptom exists for an object, the problem exists and requires that you take action to solve it. When an alert occurs, vRealize Operations Manager presents the triggering symptoms, so that you can evaluate the object in your environment, and with recommendations for how to resolve the alert.

To assess objects for symptoms, you can include symptoms packages in your policy for metrics and super metrics, properties, message events, and faults. You can enable or disable the symptoms to determine the criteria that the policy uses to assess and evaluate the data collected from the objects to which the policy applies. You can also override the threshold, criticality, wait cycles, and cancel cycles.

The Symptoms pane displays the name of the symptom, the associated management pack adapter, object type, metric or property type, a definition of the trigger such as for CPU usage, the state of the symptom, and the trigger condition. To view a specific set of symptoms in the package, you can select the adapter type, object type, metric or property type, and the state of the symptom.

When a symptom is required by an alert, the state of the symptom is enabled, but is dimmed so that you cannot modify it. The state of a required symptom includes an information icon that you can hover over to identify the alert that required this symptom.

## Where You Modify the Policy Symptom Definitions

To modify the policy package of symptoms, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy, or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left, click **Alert / Symptom Definitions**. The alert definitions and symptom definitions for the selected object types appear in the workspace.

**Table 3-22. Symptom Definitions in the Add or Edit Monitoring Policy Workspace**

Option	Description
Actions	Select one or more symptom definitions and select enable, disable, or inherit to change the state for this policy.
Filter options	<p>Deselect the options in the <b>Type</b> and <b>State</b> drop-down menus, to narrow the list of symptom definitions.</p> <ul style="list-style-type: none"> <li>■  Enabled. Indicates that a symptom definition will be included.</li> <li>■  Enabled (Force). Indicates state change due to a dependency.</li> <li>■  Disabled. Indicates that a symptom definition not be included.</li> <li>■  Inherited. Indicates that the state of this symptom definition is inherited from the base policy and will be included.</li> <li>■  Inherited. Indicates that the state of this symptom definition is inherited from the base policy and will not be included.</li> </ul> <p>Type determines whether symptom definitions that apply to HT and DT metrics, properties, events such as message, fault, and metric, and smart early warnings appear in the list.</p> <p>State determines whether enabled, disabled, and inherited symptom definitions appear in the symptom definition list.</p>
Object Type	Filters the symptom definitions list by object type
Page Size	The number of symptom definitions to list per page.
Filter	Locate data in the symptom definition list.
Symptom Definitions data grid	<p>Displays information about the symptom definitions for the object types. The full name for Symptom Definition appears in a tooltip when you hover the mouse over the Symptom Definition name.</p> <ul style="list-style-type: none"> <li>■ <b>Name.</b> Symptom definition name as defined in the list of symptom definitions in the Content area.</li> <li>■ <b>Adapter.</b> Data source type for which the alert is defined.</li> <li>■ <b>Object Type.</b> Type of object to which the alert applies.</li> <li>■ <b>Type.</b> Object type on which the symptom definition must be evaluated.</li> <li>■ <b>Trigger.</b> Static or dynamic threshold, based on the number of symptom definitions, the object type and metrics selected, the numeric value assigned to the symptom definition, the criticality of the symptom, and the number of wait and cancel cycles applied to the symptom definition.</li> <li>■ <b>State.</b> Symptom definition state, either enabled, disabled, or inherited from the base policy.</li> <li>■ <b>Condition.</b> Enables action on the threshold. When set to <b>Override</b>, you can change the threshold. Otherwise set to default.</li> <li>■ <b>Threshold.</b> To change the threshold, you must set the State to <b>Enabled</b>, set the condition to <b>Override</b>, and set the new threshold in the Override Symptom Definition Threshold dialog box.</li> </ul>

If you do not configure the package, the policy inherits the settings from the selected base policy.

## Custom Profiles Details

Custom profiles show how many more of a specified object can fit in your environment depending on the available capacity and object configuration. You can enable or disable custom profiles for your policy.

### Where You Set the Policy Custom Profiles

To apply the policy to object groups, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Custom Profiles**.

**Table 3-23. Custom Profiles Options**

Option	Description
Actions	Select one or more profiles and select enable, disable, or inherit to change the state for this policy.
Filter options	<p>Deselect the options in the <b>State</b> drop-down menu, to narrow the list of attributes.</p> <ul style="list-style-type: none"> <li>■  Enabled. Indicates that a profile will be calculated.</li> <li>■  Enabled (Force). Indicates state change due to a dependency.</li> <li>■  Disabled. Indicates that a profile not be calculated.</li> <li>■  Inherited. Indicates that the state of this profile is inherited from the base policy and will be calculated.</li> <li>■  Inherited. Indicates that the state of this profile is inherited from the base policy and will not be calculated.</li> </ul>
Object Type	Filters the profiles list by object type.

## Apply Policy to Groups Details

You can assign your local policy to one or more groups of objects to have VMware vRealize Operations Manager analyze those objects according to the settings in your policy, trigger alerts when the defined threshold levels are violated, and display the results in your dashboards, views, and reports.

### How the Apply Policy to Groups Workspace Works

When you create a policy, or modify the settings in an existing policy, you apply the policy to one or more object groups. VMware vRealize Operations Manager uses the settings in the policy to analyze and collect data from the associated objects, and displays the data in dashboards, views, and reports.

### Where You Apply a Policy to Groups

To apply the policy to object groups, click **Administration**, click **Policies**, click the **Policy Library** tab, and click the plus sign to add a policy or click the pencil to edit a policy. In the Add or Edit Monitoring policy workspace, on the left click **Apply Policy to Groups**.

### Apply Policy to Groups Options

To apply the policy to groups of objects, select the check box for the object group in the workspace.

You can then view the details about each object group associated with the policy. Select **Policies > Active Policies > Related Objects > Groups**, click an object group in the list of groups, and view the summary in the Details pane.

## Configuring Super Metrics

The super metric is a mathematical formula that contains one or more metrics. It is a custom metric that you design to help track combinations of metrics, either from a single object or from multiple objects. If a single metric cannot tell you what you need to know about the behavior of your environment, you can define a super metric.

After you define it, you assign the super metric to one or more object types. This action calculates the super metric for the objects in that object type and simplifies the metrics display. For example, if you define a super metric that calculates the average CPU usage on all virtual machines, and you assign the super metric to a cluster, the average CPU usage on all virtual machines in that cluster is reported as a super metric for the cluster.

When the super metric attribute is enabled in a policy, you can also collect super metrics from a group of objects associated with a policy.

Because super metric formulas can be complex, plan your super metric before you build it. The key to creating a super metric that alerts you to the expected behavior of your objects is knowing your own enterprise and data. Use this checklist to help identify the most important aspects of your environment before you begin to configure a super metric.

**Table 4-1. Designing a Super Metric Checklist**

<input type="checkbox"/> Determine the objects that are involved in the behavior to track.	When you define the metrics to use, you can select either specific objects or object types. For example, you can select the specific objects VM001 and VM002, or you can select the object type virtual machine.
<input type="checkbox"/> Determine the metrics to include in the super metric.	If you are tracking the transfer of packets along a network, the metrics are packets in and packets out because you are interested in the ration of those metrics. In another common use of super metrics, the metrics might be the average CPU usage or average memory usage of the object type you select.
<input type="checkbox"/> Decide how to combine or compare the metrics.	For example, to find the ratio of packets in to packets out, you must divide the two metrics. If you are tracking CPU usage for an object type, you might want to determine the average use, or you might want to determine what the highest or lowest use is for any object of that type. In more complex scenarios, you might need a formula that uses constants or trigonometric functions.

<input type="checkbox"/> Decide where to assign the super metric.	You define the objects to track in the super metric, then assign the super metric to the object type that contains the objects being tracked. To monitor all the objects in a group, enable the super metric in the policy, and apply the policy to the object group.
<input type="checkbox"/> Determine the policy to which you add the super metric.	After you create the super metric, you add it to a policy. For more information, refer to <a href="#">Policy Workspace in vRealize Operations Manager</a> .
<input type="checkbox"/> Familiarize yourself with operators and functions.	For information about operators and functions, refer to <a href="#">#unique_222</a> .

## What Else Can You Do With Super Metrics

- Generate a system audit report to see the super metrics in your environment. For more information, refer to [#unique\\_223](#).
- Define symptoms based on super metrics to create alert definitions to notify you of the performance of objects in your environment. For more information, refer to [About Metrics and Super Metrics Symptoms](#).
- Learn about the use of super metrics in policies. For more information, refer to [Policy Workspace in vRealize Operations Manager](#).
- Use OPS CLI commands to import, export, configure, and delete super metrics. For more information, refer to the OPS CLI documentation.
- Create a custom set of metrics to display metric-related widgets. You can configure one or more files that define different sets of metrics for a particular adapter and object types so that the supported widgets are populated based on the configured metrics and selected object type. For more information, refer to [Manage Metric Configuration](#).

This chapter includes the following topics:

- [Create a Super Metric](#)
- [Enhancing Your Super Metrics](#)
- [Exporting and Importing a Super Metric](#)

## Create a Super Metric

Create a super metric when you want to check the health of your environment, but cannot find a suitable metric to perform the analysis.

### Procedure

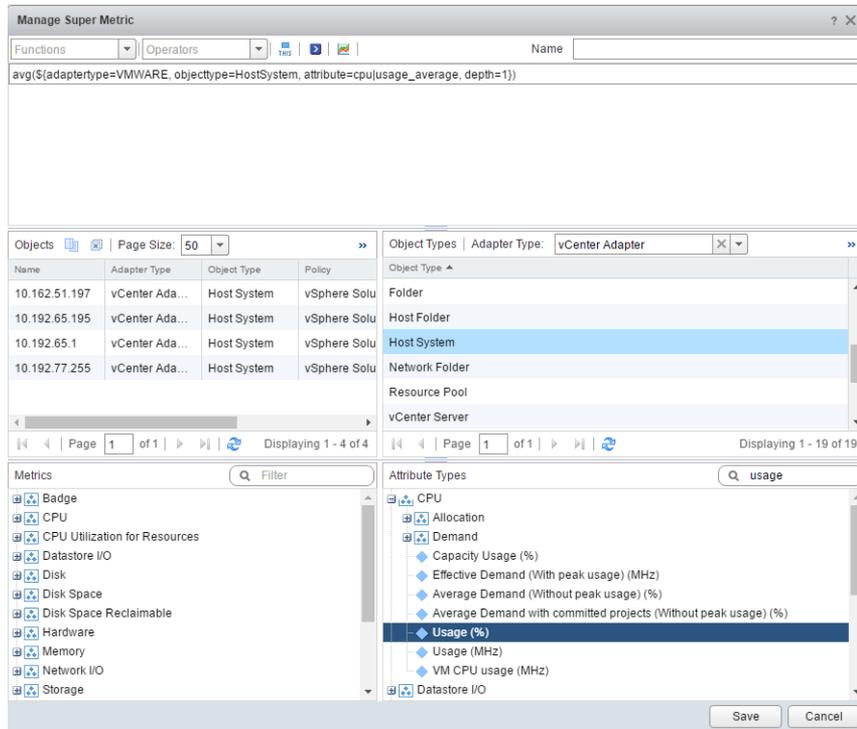
- 1 Select **Content > Super Metrics** and click the **Add** icon.
- 2 Enter a meaningful name for the super metric such as **SM-AvgVMCPUUsage%** in the **Name** text box.

### 3 Define the formula for the super metric.

Select each function or operator to use and the metrics or attribute types to use in each function or with each operator. For example, to add a super metric that captures average CPU usage across all virtual machines, perform the following tasks.

- a For Function, select **avg**.
- b In the **Operators** text box, select the left parenthesis, then select the right parenthesis. Click between the two parentheses to position your cursor in the formula.
- c In the **Adapter Type** text box of the Object Types pane, select **vCenter Adapter**.
- d Click the **This object** icon, and from the list of object types, select **Virtual Machine**.  
If the **This object** icon is not selected, the super metric function displays the object with a long description.
- e In the **Attribute Types** pane, expand the CPU category, scroll down, and double-click the **Usage (%)** metric.

The formula appears as a mathematical function. To view the formula in a textual format, click the **Show Formula Description** icon. If the formula syntax is wrong, an error message appears. The formula ends with `depth=1`. With `depth=1`, you assign the super metric to an object type that is one level above virtual machines in the relationship chain so that the super metric appears as a metric for that object type. With `depth=2`, you assign the super metric to an object type that is two levels above virtual machines, for example a Cluster.



- 4 To assign the super metric to an object type at `depth=1`, type 2 instead of 1, so that `depth=2` is displayed.

5 Check that the super metric formula has been created correctly.

- a Click the **Visualize Super Metric** icon.
- b In the Objects pane, double-click one of the objects listed.

A metric graph is displayed showing values of the metric collected for the object. Verify that the graph shows values over time.

The screenshot shows the 'Manage Super Metric' window. The formula bar contains: `avg($[adaportype=VMWARE, objecttype=HostSystem, attribute=cputusage_average, depth=1])`. The 'Objects' table lists four objects, all of type 'Host System' under 'vCenter Adapter'. The object '10.192.65.195' is selected. The 'Object Types' pane on the right shows a hierarchy where 'Host System' is selected. The graph at the bottom shows a flat line at 0 for the selected object, with a time axis from 09:00 AM to 02:30 PM.

6 Click **Save**.

7 Associate the super metric with an object so that vRealize Operations Manager calculates the super metrics for the target objects and displays it as a metric for the object type.

- a In the Super Metrics workspace, select the super metric.
- b In the **Object Types** tab, click the **Add** icon.
- c In the Select Object Type text box, select the required object. For example, if you created your super metric for Host Systems under the vCenter Adapter, expand **vCenter Adapter**, and select **Host Systems**.
- d Click **Select**.

After one collection cycle has completed, the super metric appears on each of the objects of the specified object type. For example, if you defined the super metric to calculate average CPU usage across all virtual machines, and the super metric is assigned to the Host System object type. After one collection cycle has completed, the super metric appears as a super metric on each host.

## What to do next

In the **Policies > Edit Policy > Attributes** workspace, you must select and enable each super metric. See [Custom Policies](#). Wait at least one collection cycle for the super metric to start collecting and processing data. Then review your super metric in the **All Metrics** tab.

## Enhancing Your Super Metrics

vRealize Operations Manager enables you to enhance your super metric by using clauses and resource entry aliasing.

### Where Clause

The where clause checks whether a particular metric value should be used in the super metric. Use this clause to point to a different metric of the same object, such as

```
where = "metric_group|my_metric > 0.
```

For example:

```
count({adaptertype = ExampleAdapter, objecttype = ExampleObject, metric = ExampleGroup|Rating, depth=2, where = "==1"})
```

### Resource Entry Aliasing

Resource entries are used to retrieve metric data from vRealize Operations Manager for super metric computation. A resource entry is the part of an expression which starts with **\$** followed by a **{..}** block. When computing a super metric, you may have to use the same resource entry multiple times. If you need to make changes to your computation, the changes have to be made to each and every resource entry, which may lead to errors. Use resource entry aliasing to rewrite the expression.

The following example, shows a resource entry that has been used twice.

```
(min({adapterkind=VMWARE, resourcekind=HostSystem, attribute= cpu|demand|active_longterm_load, depth=5, where=">=0"}) + 0.0001)/(max({adapterkind=VMWARE, resourcekind=HostSystem, attribute=cpu|demand|active_longterm_load, depth=5, where=">=0"}) + 0.0001)"
```

Using resource entry aliasing, you can write the expression like this. The output of both expressions are the same.

```
(min({adapterkind=VMWARE, resourcekind=HostSystem, attribute= cpu|demand|active_longterm_load, depth=5, where=">=0"} as cpuload) + 0.0001)/(max(cpuload) + 0.0001)"
```

Follow these guidelines when you use resource entry aliasing:

- To create the alias, the resource entry should be followed by **as** and then **alias:name**. For example: **{...} as alias\_name**.
- The alias cannot contain the **()[]+-%/|&!=<>,?:\$** special characters, and cannot start with a digit.
- An alias name, like all names in super metric expressions, is case-insensitive.

- Use of an alias name is optional. You can define the alias, and not use it in an expression.
- You cannot specify the same alias name more than once. For example:  
`${resource1,...} as r1 + ${resource2,...} as R1.`
- You can specify multiple aliases for the same resource entry. For example: `${...} as a1 as a2.`

## Conditional Expression ?: Ternary Operators

You can use a ternary operator in an expression to execute conditional expressions.

For example: `expression_condition ? expression_if_true : expression_if_false.`

The result of the conditional expression is converted to a number. If the value is not 0 then the condition is assumed as true.

For example: `-0.7 ? 10 : 20` results in 10. `2 + 2 / 2 - 3 ? 4 + 5 / 6 : 7 + 8` results in 15 (7 + 8).

Depending on the condition, either `expression_if_true` or `expression_if_false` is executed, but not both of them. This enables you to write expressions such as,

`${this, metric=cpu|demandmhz} as a != 0 ? 1/a : -1.` A ternary operator can contain other operators in all its expressions, including other ternary operators.

For example: `!1 ? 2 ? 3 : 4 : 5` results in 5.

## Exporting and Importing a Super Metric

You can export a super metric from one vRealize Operations Manager instance and import it to another vRealize Operations Manager instance. For example, after developing a super metric in a test environment, you can export it from the test environment and import it use in a production environment.

If the super metric to import contains a reference to an object that does not exist in the target instance, the import fails. vRealize Operations Manager returns a brief error message and writes detailed information to the log file.

### Procedure

- 1 Export a super metric.
  - a Select **Content > Super Metrics**.
  - b Select the super metric to export and click the **Export Selected Super Metric** actions icon.  
vRealize Operations Manager creates a super metric file, for example, `SuperMetric.json`.
  - c Download the super metric file to your computer.

## 2 Import a super metric.

- a Select **Content > Super Metrics** and click the **Import Super Metric** actions icon.
- b (Optional). If the target instance has a super metric with the same name as the super metric you are importing, you can either overwrite the existing super metric or skip the import, which is the default.

# Configuring Objects

Using the power of object management, including metrics and alerts - some prepackaged into dashboards and policies, others that you combine into custom monitoring tools - you'll keep a close watch on the objects, applications and systems that must stay up and running.

vRealize Operations Manager discovers objects in your environment and makes them available to you. With the information that vRealize Operations Manager provides, you can quickly access and configure any object. For example, you can check if a datastore is connected or providing data, or you can power on a virtual machine.

This chapter includes the following topics:

- [Object Discovery](#)

## Object Discovery

Its ability to monitor and collect data on objects in your systems environment makes vRealize Operations Manager a critical tool in maintaining system uptime and ensuring ongoing good health for all system resources from virtual machines to applications to storage - across physical, virtual and cloud infrastructures.

Following are examples of objects that can be monitored.

- vCenter Server
- Virtual machines
- Servers/hosts
- Compute resources
- Resource pools
- Data centers
- Storage components
- Switches
- Port groups
- Datastores

## Adapters – Key to Object Discovery

vRealize Operations Manager collects data and metrics from objects using adapters, the central components of management packs, which in turn make up vRealize Operations Manager solutions. When you configure the vSphere Solution, for example, you create adapter instances customized for your environment with unique names, port numbers, and so on. You must create an adapter instance for each vCenter Server in your deployment.

Locate existing adapters in the UI as follows: **Home > Administration > Solutions**.

As shown in the screenshot, the Solutions screen lists available solutions at the top of the screen. When you select a solution, the available adapters appear in the lower half of the screen. Existing adapter instances related to each adapter are listed in the second column.

Name	Description	Version	Provided by
Management Pack for NSX	Manages NSX-vSphere objects, Inclu...	3...	VMware Inc.
EMC Avamar Adapter	Manages EMC Avamar system	4...	EMC

Adapter Type	Adapter Instance Name	Credential name	Collector
NSX-vSphere Adapter	nsx_10.23.23.83	nsx_10.23.23.83	vRealize Operations M...
NSX-vSphere Adapter	10.26.135.205	nsx_10.26.135.205_new	vRealize Operations M...

For complete information on configuring management packs and adapters, see [Chapter 1 Connecting vRealize Operations Manager to Data Sources](#)

When you create a new adapter instance, it begins discovering and collecting data from the objects designated by the adapter, and notes the relationships between them. Now you can begin to manage your objects.

## About Objects

Objects are the structural components of your mission-critical IT applications: virtual machines, datastores, virtual switches and port groups are examples of objects.

Because downtime equals cost - in unused resources and lost business opportunities - it's crucial that you successfully identify, monitor and track objects in your environment. The goal is to proactively isolate, troubleshoot and correct problems even before users are aware that anything is wrong.

When a user actually reports an issue, the solution should be quick and comprehensive.

For a complete list of objects that can be defined in vRealize Operations Manager refer to [Object Discovery](#).

vRealize Operations Manager gives you visibility into objects including applications, storage and networks across physical, virtual and cloud infrastructures through a single interface that relates performance information to positive or negative events in the environment.

## Managing Objects

When you monitor a large infrastructure, the number of objects and corresponding metrics in vRealize Operations Manager grows rapidly, especially as you add solutions that extend dynamic monitoring and alerts to more parts of your infrastructure. vRealize Operations Manager gives you ample tools to stay abreast of events and issues.

### Adding Objects and Configuring Object Relationships

vRealize Operations Manager automatically discovers objects and their relationships once you create an adapter instance. You have the added ability to manually add any objects that you want monitored and to configure object relationships using abstract concepts rather than the connections recorded by vRealize Operations Manager. Where vRealize Operations Manager might discover the classic parent-child relationships between objects, you can create relationships between objects that might not normally be related. For example, you could configure all the datastores supporting a company department to be related.

When objects are related, a problem with one object appears as an anomaly on related objects. So object relationships can help you to identify problems in your environment quickly. The object relationships that you create are called custom groups.

### Custom Groups

To create an automated management system you need some way to organize objects so that you can quickly gain insights. You can achieve a high level of automation using custom groups. You have multiple options for tailoring group attributes to support your monitoring strategy.

For example, you can designate a group either to be static or to be updated automatically with membership criteria that you designate. Consider a non-static group of all virtual machines that are powered on and have OS type Linux. When you power on a new Linux VM, it is automatically added to the group and the policy is applied.

For additional flexibility, you can also specify individual objects to be always included or excluded from a given custom group. Or you can have a different set of alerts and capacity calculations for your production environment versus your testing environments.

### Managing Applications

vRealize Operations Manager allows you to create containers or objects that can contain a group of virtual machines or other objects in different structural tiers. This new application can then be managed as a single object, and have health badges and alarms aggregated from the child objects of the group.

For example, the system administrator of an online training system might request that you monitor components in the Web, application and database tiers of the training environment. You build an application that groups related training objects together in each tier. If a problem occurs with one of the objects, it is highlighted in the application display and you can investigate the source of the problem

## The Power of Object Management

Using the power of object management, including metrics and alerts - some prepackaged into dashboards and policies, others that you combine into custom monitoring tools - you'll keep a close watch on the objects, applications and systems that must stay up and running.

## Managing Objects in Your Environment

An object is the individual managed item in your environment for which vRealize Operations Manager collects data, such as a router, switch, database, virtual machine, host, and vCenter Server instances.

vRealize Operations Manager requires specific information about each object. When you configure an adapter instance, vRealize Operations Manager performs object discovery to start collecting data from the objects with which the adapter communicates.

An object can be a single entity, such as a database, or a container that holds other objects. For example, if you have multiple Web servers, you can define a single object for each Web server and define a separate container object to hold all of the Web server objects. Groups and applications are types of containers.

You categorize your objects using tags, so that you can easily find, group, or filter them later. A tag type can have multiple tag values. You or vRealize Operations Manager assigns objects to tag values. When you select a tag value, vRealize Operations Manager displays the objects associated with that tag. For example, if a tag type is Lifecycle and tag values are Development, Test, Pre-production, and Production, you might assign virtual machine objects VM1, VM2, or VM3 in your environment to one or more of these tag values, depending on the virtual machine function.

## Adding an Object to Your Environment

You might want to add an object by providing its information to vRealize Operations Manager. For example, some solutions cannot discover all the objects that might be monitored. For these solutions, you must either use manual discovery or manually add the object.

When you add an individual object, you provide specific information about it, including the kind of adapter to use to make the connection and the connection method. For example, an SNMP adapter does not know the location of the SNMP devices that you want to monitor. You can use manual discovery to perform a port scan through an IP range. If port scans are not allowed on the network for security reasons, you must add the devices manually.

### Prerequisites

Verify that an adapter is present for the object you plan to add. See the *vRealize Operations Manager vApp Deployment and Configuration Guide*.

### Procedure

- 1 Select **Administration > Inventory Explorer**.
- 2 On the toolbar, click the plus sign.

### 3 Provide the required information.

Option	Description
<b>Display name</b>	Enter a name for the object. For example, enter <b>SNMP-Switch1</b> .
<b>Description</b>	Enter any description. For example, enter <b>Switch monitored with SNMP adapter</b>
<b>Adapter type</b>	Select an adapter type. For example, select <b>SNMP Adapter</b> .
<b>Adapter instance</b>	Select an adapter instance.
<b>Object type</b>	Select an object type. For an SNMP adapter, select an MIB file. vRealize Operations Manager uses the MIB file to determine what data is available on the switch. When you select the object type, the dialog box selections change to include information you provide so that vRealize Operations Manager can find and connect with the selected object type.
<b>Host IP address</b>	Enter the host IP. For example, enter the IP address of the switch.
<b>Port number</b>	Accept the default port number or enter a new value. For the SNMP adapter, this port is the SNMP management port number.
<b>Credential</b>	Select the Credential, or click the plus sign to add new login credentials for the object.
<b>Collection interval</b>	Enter the collection interval, in minutes. For example, if you expect the switch to generate performance data every 5 minutes, set the collection interval to 5 minutes.
<b>Dynamic Thresholding.</b>	Accept the default, Yes.

### 4 Click **OK** to add the object.

SNMP-Switch1 appears in the Inventory Explorer as an MIB object type for the SNMP adapter type.

#### What to do next

For each new object, vRealize Operations Manager assigns tag values for its collector and its object type. Sometimes, you might want to assign other tags.

## Configuring Object Relationships

vRealize Operations Manager shows the relationship between objects in your environment. Most relationships are automatically formed when the objects are discovered by an installed adapter. In addition, you can use vRealize Operations Manager to create relationships between objects that might not normally be related.

Objects are related physically, logically, or structurally.

- Physical relationships represent how objects connect in the physical world. For example, virtual machines running on a host are physically related.
- Logical relationships represent business silos. For example, all the storage objects in an environment are related to one another.
- Structural relationships represent a business value. For example, all the virtual machines that support a database are structurally related.

Solutions use adapters to monitor the objects in your environment so that physical relationship changes are reflected in vRealize Operations Manager. To maintain logical or structural relationships, you can use vRealize Operations Manager to define the object relationships. When objects are related, a problem with one object appears as an anomaly on related objects. So object relationships can help you to identify problems in your environment quickly.

## Creating and Assigning Tags

A large enterprise can have thousands of objects defined in vRealize Operations Manager. Creating object tags and tag values makes it easier to find objects and metrics in vRealize Operations Manager. With object tags, you select the tag value assigned to an object and view the list of objects that are associated with that tag value.

A tag is a type of information, such as Adapter Types. Adapter Types is a predefined tag in vRealize Operations Manager. Tag values are individual instances of that type of information. For example, when vRealize Operations Manager discovers objects using the vCenter Adapter, it assigns all the objects to the vCenter Adapter tag value under the Adapter Types tag.

You can assign any number of objects to each tag value, and you can assign a single object to tag values under any number of tags. You typically look for an object by looking under its adapter type, its object type, and possibly other tags.

If an object tag is locked, you cannot add objects to it. vRealize Operations Manager maintains locked object tags.

- [Predefined Object Tags](#)

vRealize Operations Manager includes several predefined object tags. It creates values for most of these tags and assigns objects to the values.

- [Add an Object Tag and Assign Objects to the Tag](#)

An object tag is a type of information, and a tag value is an individual instance of that type of information. If the predefined object tags do not meet your needs, you can create your own object tags to categorize and manage objects in your environment. For example, you can add a tag for cloud objects and add tag values for different cloud names. Then you can assign objects to the cloud name.

- [Use a Tag to Find an Object](#)

The quickest way to find an object in vRealize Operations Manager is to use tags. Using tags is more efficient than searching through the entire object list.

### Predefined Object Tags

vRealize Operations Manager includes several predefined object tags. It creates values for most of these tags and assigns objects to the values.

For example, when you add an object, vRealize Operations Manager assigns it to the tag value for the collector it uses and the kind of object that it is. It creates tag values if they do not already exist.

If a predefined tag has no values, there is no object of that tag type. For example, if no applications are defined in your vRealize Operations Manager instance, the applications tag has no tag values.

Each tag value appears with the number of objects that have that tag. Tag values that have no objects appear with the value zero. You cannot delete the predefined tags or tag values that vRealize Operations Manager creates.

**Table 5-1. Predefined Tags**

Tag	Description
Collectors (Full Set)	Each defined collector is a tag value. Each object is assigned to the tag value for the collector that it uses when you add the object to vRealize Operations Manager. The default collector is vRealize Operations Manager Collector-vRealize.
Applications (Full Set)	Each defined application is a tag value. When you add a tier to an application, or an object to a tier in an application, the tier is assigned to that tag value.
Maintenance Schedules (Full Set)	Each defined maintenance schedule is a tag value, and objects are assigned to the value when you give them a schedule by adding or editing them.
Adapter Types	Each adapter type is a tag value, and each object that uses that adapter type is given the tag value.
Adapter Instances	Each adapter instance is a tag value, and each object is assigned the tag value for the adapter instance or instances through which its metrics are collected.
Object Types	Each type of object is a tag value, and each object is assigned to the tag value for its type when you add the object.
Recently Added Objects	The last day, seven days, 10 days, and 30 days have tag values. Objects have this tag value as long as the tag value applies to them.
Object Statuses	Tag value assigned to objects that are not receiving data.
Collection States	Tag value assigned to indicate the object collection state, such as collecting or not collecting.
Health Ranges	Good (green), Warning (yellow), Immediate (orange), Critical (red), and Unknown (blue) health statuses have tag values. Each object is assigned the value for its current health status.
Entire Enterprise	The only tag value is Entire Enterprise Applications. This tag value is assigned to each application.
Licensing	Tag values are License Groups found under <b>Administration &gt; Licensing. Objects</b> are assigned to the license groups during vRealize Operations Manager installation.
Untag	Drag an object to this tag to delete the tag assignment.

### Add an Object Tag and Assign Objects to the Tag

An object tag is a type of information, and a tag value is an individual instance of that type of information. If the predefined object tags do not meet your needs, you can create your own object tags to categorize and manage objects in your environment. For example, you can add a tag for cloud objects and add tag values for different cloud names. Then you can assign objects to the cloud name.

## Prerequisites

Become familiar with the predefined object tags.

## Procedure

- 1 Select **Administration > Inventory Explorer**.
- 2 Click the **Manage Tags** icon above the list of tags.
- 3 Click the **Add New Tag** icon to add a new row and type the name of the tag in the row.  
For example, type **Cloud Objects** and click **Update**.
- 4 With the new tag selected, click the **Add New Tag Value** icon to add a new row and type the name of the value in the row.  
For example, type **Video Cloud** and click **Update**.
- 5 Click **OK** to add the tag.
- 6 Click the tag to which you want to add objects to display the list of object tag values.  
For example, click **Cloud Objects** to display the Video Cloud object tag value.
- 7 Drag objects from the list in the right pane of the Inventory Explorer onto the tag value name.  
You can press Ctrl+click to select multiple individual objects or Shift+click to select a range of objects.  
For example, if you want to assign datacenters that are connected through the vCenter Adapter, type **vCenter** in the search filter and select the datacenter objects to add.

## Use a Tag to Find an Object

The quickest way to find an object in vRealize Operations Manager is to use tags. Using tags is more efficient than searching through the entire object list.

Tag values that can also be tags are Applications and Object Types. For example, the Object Types tag has values for each object that is in vRealize Operations Manager, such as Virtual Machine, which includes all the virtual machine objects in your environment. Each of these virtual machines is also a tag value for the Virtual Machine tag. You can expand the tag value list to select the value for which you want to see objects.

## Procedure

- 1 Select **Administration > Inventory Explorer**.
- 2 In the tag list in the center pane, click a tag for an object with an assigned value.  
When you click a tag, the list of values expands under the tag. The number of objects that is associated with each value appears next to the tag value.  
A plus sign next to a tag value indicates that the value is also a tag and that it contains other tag values. You can click the plus sign to see the subvalues.

### 3 Select the tag value.

The objects that have that tag value appear in the pane on the right. If you select multiple tag values, the objects in the list depend on the values that you select.

Tag Value Selection	Objects Displayed
More than one value for the same tag	The list includes objects that have either value. For example, if you select two values of the Object Types tag, such as Datacenter and Host System, the list shows objects that have either value.
Values for two or more different tags	The list includes only objects that have all of the selected values. For example, if you select two values of the Object Types tag, such as Datacenter and Host System, and you also select an adapter instance such as vC-1 of the vCenter Adapter instance tag, only Datacenter or Host System objects associated with vC-1 appear in the list. Datacenter or Host System objects associated with other adapter instances do not appear in the list, nor do objects that are not Datacenter or Host System objects.

### 4 Select the object from the list.

## Managing Custom Object Groups in VMware vRealize Operations Manager

A custom object group is a container that includes one or more objects. vRealize Operations Manager uses custom groups to collect data from the objects in the group, and report on the data collected.

### Why Use Custom Object Groups?

You use groups to categorize your objects and have vRealize Operations Manager collect data from the groups of objects and display the results in dashboards and views according to the way you define the data to appear.

You can create static groups of objects, or dynamic groups with criteria that determines group membership as vRealize Operations Manager discovers and collects data from new added to the environment.

vRealize Operations Manager provides commonly used object group types, such as World, Environment, and Licensing. vRealize Operations Manager uses the object group types to categorize groups of objects. You assign a group type to each group so that you can categorize and organize the groups of objects that you create.

### Types of Custom Object Groups

When you create custom groups, you can use rules to apply dynamic membership of objects to the group, or you can manually add the objects to the group. When you add an adapter to vRealize Operations Manager, the groups associated with the adapter become available in vRealize Operations Manager.

- Dynamic group membership. To dynamically update the membership of objects in a group, define rules when you create a group. vRealize Operations Manager adds objects to the group based on the criteria that you define.
- Mixed membership, which includes dynamic and manual.

- Manual group membership. From the inventory of objects, you select objects to add as members to the group.
- Groups associated with adapters. Each adapter manages the membership of the group. For example, the vCenter Server adapter adds groups such as datastore, host, and network, for the container objects in the vSphere inventory. To modify these groups, you must do so in the adapter.

Administrators of vRealize Operations Manager can set advanced permissions on custom groups. Users who have privileges to create groups can create custom groups of objects and have vRealize Operations Manager apply a policy to each group to collect data from the objects and report the results in dashboards and views.

When you create a custom group, and assign a policy to the group, vRealize Operations Manager can use the criteria defined in the applied policy to collect data from and analyze the objects in the group. vRealize Operations Manager reports on the status, problems, and recommendations for those objects based on the settings in the policy.

---

**Note** Only custom groups defined explicitly by users can be exported from or imported to vRealize Operations Manager. Users are able to export or import multiple custom groups. Once an import function has been executed, the user must check to determine if a policy or policies should be associated with the imported group. Export-import operations are available for user defined (created explicitly by user) custom groups only.

---

## How Policies Help vRealize Operations Manager Report On Object Groups

vRealize Operations Manager analyzes the objects in the object group and reports on the workload, capacity, stress, anomalies, and faults of the object group, among other attributes.

When you apply a policy to an object group, vRealize Operations Manager uses threshold settings, metrics, super metrics, attributes, properties, alert definitions, and problem definitions that you enabled in the policy to collect data from the objects in the group, and report the results in dashboards and views.

When you create a new object group, you have the option to apply a policy to the group.

- To associate a policy with the custom object group, select the policy in the group creation wizard.
- To not associate a specific policy with the object group, leave the policy selection blank. The custom object group will be associated with the default policy. If the default policy changes, this object group will be associated with the new default policy.

vRealize Operations Manager applies policies in priority order, as they appear on the Active Policies tab. When you establish the priority for your policies, vRealize Operations Manager applies the configured settings in the policies according to the policy rank order to analyze and report on your objects. To change the priority of a policy, you click and drag a policy row. The default policy is always kept at the bottom of the priority list, and the remaining list of active policies starts at priority 1, which indicates the highest priority policy. When you assign an object to be a member of multiple object groups, and you assign a different policy to each object group, vRealize Operations Manager associates the highest ranking policy with that object.

## User Scenario: Creating Custom Object Groups

As a system administrator, you must monitor the capacity for your clusters, hosts, and virtual machines. vRealize Operations Manager must monitor them at different service levels to ensure that these objects adhere to the policies established for your IT department, and discover and monitor new objects added to the environment. You will have vRealize Operations Manager apply policies to the object groups to analyze, monitor, and report on the status of their capacity levels.

To have vRealize Operations Manager monitor the capacity levels for your objects to ensure that they adhere to your policies for your service levels, you will categorize your objects into Platinum, Gold, and Silver object groups to support the service tiers established.

You will create a group type, and create dynamic object groups for each service level. You will define membership criteria for each dynamic object group to have vRealize Operations Manager keep the membership of objects current. For each dynamic object group, you will assign the group type, and add criteria to maintain membership of your objects in the group. To associate a policy with the custom object group, you can select the policy in the group creation wizard.

### Prerequisites

- Know the objects that exist in your environment, and the service levels that they support.
- Understand the policies required to monitor your objects.
- Verify that vRealize Operations Manager includes policies to monitor the capacity of your objects.

### Procedure

- 1 To create a group type to identify service level monitoring, select **Content** and click **Group Types**.
- 2 On the Group Types toolbar, click the plus sign and type **Service Level Capacity** for the group type.

Your group type appears in the list.

- 3 Select **Environment**, and click **Custom Groups**.

A folder named Service Level Capacity appears in the list of custom groups in the navigation pane, and the Environment Overview displays the **Groups** tab.

- 4 To create a new object group, click the plus sign on the Groups toolbar.

The New Group workspace appears where you define the data and membership criteria for the dynamic group.

- a In the Name text box, type a meaningful name for the object group, such as **Platinum\_Objects**.
- b In the **Group Type** drop-down menu, select **Service Level Capacity**.

- c (Optional) In the **Policy** drop-down menu, select your service level policy that has thresholds set to monitor the capacity of your objects.

To associate a policy with the custom object group, select the policy in the group creation wizard. To not associate a specific policy with the object group, leave the policy selection blank. The custom object group will be associated with the default policy. If the default policy changes, this object group will be associated with the new default policy.

- d Select the **Keep group membership up to date** check box so that vRealize Operations Manager can discover objects that meet the criteria, and add those objects to the group.
- 5 Define the membership for virtual machines in your new dynamic object group to monitor them as platinum objects.
- a From the **Select Object** drop-down menu, select **vCenter Adapter**, and select **Virtual Machine**.
  - b From the empty drop-down menu for the criteria, select **Metrics**.
  - c From the **Pick a metric** drop-down menu, select **Disk Space** and double-click **Current Size**.
  - d From the conditional value drop-down menu, select **is less than**.
  - e From the **Metric value** drop-down menu, type **10**.
- 6 Define the membership for host systems in your new dynamic object group to monitor them as platinum objects.
- a Click **Add another criteria set**.
  - b From the **Select Object** drop-down menu, select **vCenter Adapter**, and select **Host System**.
  - c From the empty drop-down menu for the criteria, select **Metrics**.
  - d From the **Pick a metric** drop-down menu, select **Disk Space** and double-click **Current Size**.
  - e From the conditional value drop-down menu, select **is less than**.
  - f From the **Metric value** drop-down menu, type **100**.
- 7 Define the membership for cluster compute resources in your new dynamic object group.
- a Click **Add another criteria set**.
  - b From the **Select Object** drop-down menu, select **vCenter Adapter**, and select **Cluster Compute Resources**.
  - c From the empty drop-down menu for the criteria, select **Metrics**.
  - d From the **Pick a metric** drop-down menu, select **Disk Space** and double-click **capacityRemaining**.
  - e From the conditional value drop-down menu, select **is less than**.
  - f From the **Metric value** drop-down menu, type **1000**.
  - g Click **Preview** to determine whether objects already match this criteria.

- 8 Click **OK** to save your group.

When you save your new dynamic group, the group appears in the Service Level Capacity folder, and in the list of groups on the **Groups** tab.

- 9 Wait five minutes for vRealize Operations Manager to collect data from the objects in your environment.

vRealize Operations Manager collects data from the cluster compute resources, host systems, and virtual machines in your environment, according to the metrics that you defined in the group and the thresholds defined in the policy that is applied to the group, and displays the results about your objects in dashboards and views.

### What to do next

To monitor the capacity levels for your platinum objects, create a dashboard, and add widgets to the dashboard. See [Dashboards](#).

## Managing Application Groups

An application is a container construct that represents a collection of interdependent hardware and software components that deliver a specific capability to support your business. vRealize Operations Manager builds an application to determine how your environment is affected when one or more components in an application experiences problems, and to monitor the overall health and performance of the application. Object membership in an application is not dynamic. To change the application, you manually modify the objects in the container.

### Reasons to Use Applications

vRealize Operations Manager collects data from components in the application and displays the results in a summary dashboard for each application with a real-time analysis for any or all of the components. If a component experiences problems, you can see where in the application the problems arise, and determine how problems spread to other objects.

### User Scenario: Adding an Application

As the system administrator of an online training system, you must monitor components in the Web, application, and database tiers of your environment that can affect the performance of the system. You build an application that groups related objects together in each tier. If a problem occurs with one of the objects, it is reflected in the application display and you can open a summary to investigate the source of the problem further.

In your application, you add the DB-related objects that store data for the training system in a tier, Web-related objects that run the user interface in a tier, and application-related objects that process the data for the training system in a tier. The network tier might not be needed. Use this model to develop your application.

### Procedure

- 1 Click **Environment** in the left pane.

2 Click the **Applications** tab and click the plus sign.

3 Click **Basic n-tier Web App** and click **OK**.

The Application Management page that appears has two rows. Select objects from the bottom row to populate the tiers in the top row.

4 Type a meaningful name such as **Online Training Application** in the Application text box.

5 For each of the Web, application, and database tiers listed, add the objects to the Tier Objects section.

a Select a tier name. This is the tier that you populate.

b To the left of the object row, select object tags to filter for objects that have that tag value. Click the tag name once to select the tag from the list and click the tag name again to deselect the tag from the list. If you select multiple tags, objects displayed depend on the values that you select.

You can also search for the object by name.

c To the right of the object row, select the objects to add to the tier.

d Drag the objects to the Tier Objects section.

6 Click Save to save the application.

The new application appears in the list of applications on the Environment Overview Applications page. If any of the components in any of the tiers develops a problem, the application displays a yellow or red status.

#### **What to do next**

To investigate the source of the problem, click the application name and evaluate the object summary information. See the *vRealize Operations Manager User Guide*.

# Configuring Data Display

You configure the content in vRealize Operations Manager to suit your information needs, using views, reports, dashboards, and widgets.

Views display data, based on an object type. You can select from various view types to see your data from a different perspective. Views are reusable components that you can include in reports and dashboards. Reports can contain predefined or custom views and dashboards in a specified order. You build the reports to represent objects and metrics in your environment. You can customize the report layout by adding a cover page, a table of contents, and a footer. You can export the report in a PDF or CSV file format for further reference.

You use dashboards to monitor the performance and state of objects in your virtual infrastructure. Widgets are the building blocks of dashboards and display data about configured attributes, resources, applications, or the overall processes in your environment. You can also incorporate views in dashboards using the vRealize Operations Manager View Widget.

This chapter includes the following topics:

- [Widgets](#)
- [Dashboards](#)
- [Views](#)
- [Reports](#)

## Widgets

Widgets are the panes on your dashboards. You add widgets to a dashboard to create a dashboard. Widgets show information about attributes, resources, applications, or the overall processes in your environment.

You can configure widgets to reflect your specific needs. The available configuration options vary depending on the widget type. You must configure some of the widgets before they display any data. Many widgets can provide or accept data from one or more widgets. You can use this feature to set the data from one widget as filter and display related information on a single dashboard.



Configure Widgets

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_configure\\_widgets\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_configure_widgets_vrom))

## Widget Interactions

Widget interactions are the configured relationships between widgets in a dashboard where one widget provides information to a receiving widget. When you are using a widget in the dashboard, you select data on one widget to limit the data that appears in another widget, allowing you to focus on a smaller subset data.

### How Interactions Work

If you configured interactions between widget at the dashboard level, you can then select one or more objects in the providing widget to filter the data that appears in the receiving widget, allowing you to focus on data related to an object.

To use the interaction option between the widgets in a dashboard, you configure interactions at the dashboard level. If you do not configure any interactions, the data that appears in the widgets is based on how the widget is generally configured.

When you configure widget interaction, you specify the providing widget for the receiving widget. For some widgets, you can define two providing widgets, each of which can be used to filter data in the receiving widget.

For example, if you configured the Object List widget to be a provider widget for the Top-N widget, you can select one or more objects in the Object List widget and the Top-N displays data only for the selected objects.

For some widgets, you can define more than one providing widget. For example, you can configure the Metric Chart widget to receive data from a metrics provider widget and an objects providing widget. In such case, the Metric Chart widget shows data for any object that you select in the two provider widgets.

## Manage Metric Configuration

You can create a custom set of metrics to display the widgets. You can configure one or more files that define different sets of metrics for a particular adapter and object types so that the supported widgets are populated based on the configured metrics and selected object type.

### How the Metric Configuration Works

From the Metric Configuration page, you create an XML file that displays a set of metrics at a supported widget. The widgets are Metric Chart, Property List, Rolling View Chart, Scoreboard, Sparkline Chart, and Topology Graph. To use the metric configuration, you must set the widget Self Provider to **Off** and create a widget interaction with a provider widget.

### Where You Find the Metric Configuration

To manage metric configurations, in the left pane, select **Content > Manage Metric Config**.

**Table 6-1. Manage Metric Config Toolbar Options**

Option	Description
Create Configuration	Creates an empty XML file in a selected folder .
Edit Configuration	Activates a selected XML file for edit in the text box on the right.
Delete Configuration	Deletes a selected XML file.
Text box	Displays a selected XML file. You must select an XML file and click <b>Edit</b> to edit it.

## Add a Resource Interaction XML File

A resource interaction file is a custom set of metrics that you want to display in widgets that support the option. You can configure one or more files that define different sets of metrics for particular object types so that the supported widgets are populated based the configured metrics and selected object type.

The following widgets support the resource interaction mode:

- Metric Chart
- Property List
- Rolling View Chart
- Scoreboard
- Sparkline Chart
- Topology Graph

To use the metric configuration, which displays a set of metrics that you defined in an XML file, the dashboard and widget configuration must meet the following criteria:

- The dashboard **Widget Interaction** options are configured so that another widget provides objects to the target widget. For example, an Object List widget provides the object interaction to a chart widget.
- The widget **Self Provider** option is set to **Off**.
- The custom XML file in the **Metric Configuration** drop-down menu is in the `/usr/lib/vmware-vcops/tools/opsccli` directory and has been imported into the global storage using the `import` command.

If you add an XML file and later modify it, the changes might not take effect.

### Prerequisites

- Verify that you have the necessary permissions to access the installed files for vRealize Operations Manager and add files.
- Create a new files based on the existing examples. Examples are available in the following location:
  - vApp or Linux. The XML file is in `/usr/lib/vmware-vcops/tomcat-web-app/webapps/vcops-web-ent/WEB-INF/classes/resources/reskndmetrics`.

## Procedure

- 1 Create an XML file that defines the set of metrics.

For example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AdapterKinds>
  <AdapterKind adapterKindKey="VMWARE">
    <ResourceKind resourceKindKey="HostSystem">
      <Metric attrkey="sys:host/vim/vmvisor/slp|resourceMemOverhead_latest" />
      <Metric attrkey="cpu|capacity_provisioned" />
      <Metric attrkey="mem|host_contention" />
    </ResourceKind>
  </AdapterKind>
</AdapterKinds>
```

In this example, the displayed data for the host system based on the specified metrics.

- 2 Save the XML file in one of the following directories base on the operating system of your vRealize Operations Manager instance.

Operating System	File Location
vApp or Linux	/usr/lib/vmware-vcops/tools/opscli

- 3 Run the import command.

Operating System	File Location
vApp or Linux	./ops-cli.py file import reskndmetric YourCustomFilename.xml

The file is imported into global storage and is accessible from the supported widgets.

- 4 If you update an existing file and must re-import the file, append `--force` to the above import command and run it.

For example, `./vcops-cli.py file import reskndmetric YourCustomFilename.xml --force`.

### What to do next

To verify that the XML file is imported, configure one of the supported widgets and ensure that the new file appears in the drop-down menu.

## Widget Definitions List

A widget is a pane on a dashboard that contains information about configured attributes, resources, applications, or the overall processes in your environment. Widgets can provide a holistic, end-to-end view of the health of all of the objects and applications in your enterprise. If your user account has the necessary access rights, you can add and remove widgets from your dashboards.

**Table 6-2. Summary of Widgets**

<b>Widget Name</b>	<b>Description</b>
Alert List	Shows a list of alerts for the objects that the widget is configured to monitor. If no objects are configured, the list displays all alerts in your environment.
Alert Volume	Shows a trend report for the last seven days of alerts generated for the objects it is configured to monitor.
Anomalies	Shows a chart of the anomalies count for the past 6 hours.
Anomaly Breakdown	Shows the likely root causes for symptoms for a selected resource.
Capacity	Shows a chart of the Capacity values for a specific resources over the past 7 days.
Capacity Utilization	Shows the capacity or workload utilization for objects so that you can identify problems with capacity and workload. Indicates objects that are underutilized, optimal, and overutilized, and indicates why they are constrained.
Container Details	Shows the health and alert counts for each tier in a single selected container.
Container Object List	Shows a list of all defined resources and object types.
Container Overview	Shows the overall health and the health of each tier for one or more containers.
Current Policy	Shows the highest priority policy applied to a custom group.
Data Collection Results	Shows a list of all supported actions specific for a selected object.
Density	Shows the density breakdown as charts for the past 7 days for a specific resource.
DRS Cluster Settings	Shows the workload of the available clusters and the associated hosts.
Efficiency	Shows the status of the efficiency-related alerts for the objects that it is configured to monitor. Efficiency is based on generated efficiency alerts in your environment.
Environment	Lists the number of resources by object or groups them by object type.
Environment Overview	Shows the performance status of objects in your virtual environment and their relationships. You can click an object to highlight its related objects and double-click an object to view its Resource Detail page.
Environment Status	Shows statistics for the overall monitored environment.
Faults	Shows a list of availability and configuration issues for a selected resource.
Forensics	Shows how often a metric had a particular value, as a percentage of all values, within a given time period. It can also compare percentages for two time periods.
Geo	Shows where your objects are located on a world map, if your configuration assigns values to the Geo Location object tag.
Health	Shows the status of the health-related alerts for the objects that it is configured to monitor. Health is based on generated health alerts in your environment.
Health Chart	Shows health information for selected resources, or all resources that have a selected tag.
Heat Map	Shows a heat map with the performance information for a selected resource.
Mashup Chart	Brings together disparate pieces of information for a resource. It shows a health chart, an anomaly count graph, and metric graphs for key performance indicators (KPIs). This widget is typically used for a container.
Metric Chart	Shows a chart with the workload of the object over time based on the selected metrics.

Widget Name	Description
Metric Picker	Shows a list of available metrics for a selected resource. It works with any widget that can provide resource ID.
Object List	Shows a list of all defined resources.
Object Relationship	Shows the hierarchy tree for the selected object.
Object Relationship (Advanced)	Shows the hierarchy tree for the selected objects. It provides advanced configuration options.
Property List	Shows the properties and their values of an object that you select.
Reclaimable Capacity	Shows a percentage chart representing the amount of reclaimable capacity for a specific resource that has consumers.
Recommended Actions	Displays recommendations to solve problems in your vCenter Server instances. With recommendations, you can run actions on your data centers, clusters, hosts, and virtual machines.
Risk	Shows the status of the risk-related alerts for the objects that it is configured to monitor. Risk is based on generated risk alerts in your environment.
Rolling View Chart	Cycles through selected metrics at an interval that you define and shows one metric graph at a time. Miniature graphs, which you can expand, appear for all selected metrics at the bottom of the widget.
Scoreboard	Shows values for selected metrics, which are typically KPIs, with color coding for defined value ranges.
Scoreboard Health	Shows color-coded health or workload scores for selected resources.
Sparkline Chart	Shows graphs that contain metrics for an object . If all of the metrics in the Sparkline Chart widget are for an object that another widget provides, the object name appears at the top right of the widget.
Stress	Shows a weather map of the average stress over the past 6 weeks for a specific resource.
Tag Picker	Lists all defined resource tags.
Text Display	Reads text from a Web page or text file and shows the text in the user interface.
Time Remaining	Shows a chart of the Time Remaining values for a specific resources over the past 7 days.
Top Alerts	Lists the alerts most likely to negatively affect your environment based on the configured alert type and objects.
Top-N	Shows the top or bottom N number metrics or resources in various categories, such as the five applications that have the best or worth health score.
Topology Graph	Shows multiple levels of resources between nodes.
View	Shows a defined view depending on the configured resource.
Weather Map	Uses changing colors to show the behavior of a selected metric over time for multiple resources.
Workload	Shows workload information for a selected resource.

For more information about the widgets, see the vRealize Operations Manager help.

## Dashboards

Dashboards present a visual overview of the performance and state of objects in your virtual infrastructure. You use dashboards to determine the nature and timeframe of existing and potential issues with your environment. You create dashboards by adding widgets to a dashboard and configuring them.

vRealize Operations Manager collects performance data from monitored software and hardware resources in your enterprise and provides predictive analysis and real-time information about problems. The data and analysis are presented through alerts, in configurable dashboards, on predefined pages, and in several predefined dashboards.

- You can start with several predefined dashboards in vRealize Operations Manager.
- You can create extra ones that meet your specific needs using widgets, views, badges, and filters to change the focus of the information.
- You can clone and edit the predefined dashboards or start from scratch.
- To display data that shows dependencies, you can add widget interactions in dashboards.
- You can provide role-based access to various dashboards for better collaboration in teams.

**Table 6-3. vRealize Operations Manager Home Page Menus**

Menu	Description
Dashboard List	Lists all dashboards that are visible on the home page. You can use this menu for a quick navigation through your dashboards.
Actions	Available dashboard actions, such as create, edit, delete, and set as default. These actions are applied directly to the dashboard that you are on.



Create Custom Dashboards

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_create\\_dashboards\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_create_dashboards_vrom))

## Types Of Dashboards

You can use the predefined dashboards or create your own custom dashboard in vRealize Operations Manager.

### Predefined Dashboards

vRealize Operations Manager has predefined dashboards that address several key questions including how you can troubleshoot your VMs, the workload distribution of your hosts, clusters, and datastores, the capacity of your data center, and information about the VMs. You can also log details.

You can access the predefined dashboards from the Home page. Click **Dashboard List > vSphere Dashboards Library** or just **Dashboard List**.

The following are the predefined dashboards that have been added in vRealize Operations Manager:

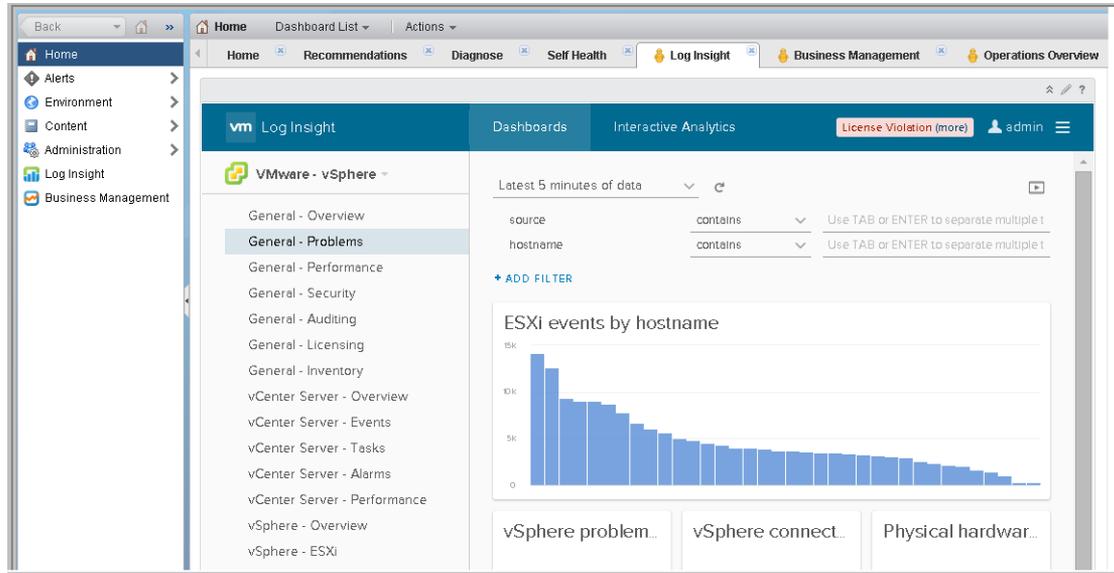
- Log Insight

- Business Management
- Getting Started
- Operations Overview
- Capacity Overview
- Troubleshoot a VM
- VM Dashboards
  - Heavy Hitter VMs
  - VM Configuration
  - VM Usage
- Infrastructure Dashboards
  - Cluster Configuration
  - Cluster Performance
  - Datastore Capacity
  - Datastore Performance
  - ESXi Configuration
  - Network Configuration

### **Log Insight Dashboard**

When vRealize Operations Manager is integrated with vRealize Log Insight, you can access the custom dashboards and content pack dashboards from the Log Insight dashboard. You can view graphs of log events in your environment, or create custom sets of widgets to access the information that matters most to you.

For more information about the Log Insight dashboard, see the [vRealize Log Insight documentation](#).



To access the Log Insight dashboard from vRealize Operations Manager, you must either:

- Configure the vRealize Log Insight adapter from the vRealize Operations Manager interface, or
- Configure vRealize Operations Manager in vRealize Log Insight.

For more information on configuring, see [Configuring vRealize Log Insight with vRealize Operations Manager](#).

## Business Management Dashboard

When vRealize Operations Manager is integrated with vRealize Business for Cloud, you can display infrastructure and cost information in the Business Management dashboard and the Business Management page.

To display infrastructure and cost information, you must configure the vRealize Business for Cloud adapter. For information about configuring this adapter, refer to [Configure vRealize Business for Cloud Adapter](#).

## Getting Started Dashboard

The Getting Started dashboard lists the predefined dashboards in one page. You can use this dashboard to understand key questions that each predefined dashboard can help you answer.

After you get familiar with the new predefined dashboards, you can disable this dashboard by clicking **Actions > Remove Dashboard from Menu**.

## Operations Overview Dashboard

The Operations Overview dashboard provides an overview of the different data centers for which you are responsible, and helps you to act on alerts to ensure that there are no underlying infrastructure problems.

You can use the dashboard widgets in several ways.

- **Inventory Summary:** Use this widget to view a summary of the overall inventory of your environment.

- **Select a Datacenter:** Use this widget to select the data center for which you want to view operational information. You can use the filter to narrow your list based on several parameters. After you identify the data center you want to view, select it. The dashboard is automatically populated with the relevant data.
- **Uptime of all Clusters:** Use this widget to view the overall health of the clusters in the data center you selected. The metric value is calculated based on the uptime of each ESXi host, when you take into account one host as the HA host. If the number displayed is less than 100%, it means that at least two hosts within the cluster were not operational for that period.
- **Alert Volume:** Use this widget to view the breakdown of alert trends based on their criticality.
- **Top-N:** You can also view a list of 15 VMs that had the highest average CPU contention, the highest use of memory, and the highest disk latency for the last 24 hours. To obtain specific data, you can manually set the time to the time of the problem. To set the time, click the **Edit Widget** icon from the title bar of the widget and edit the **Period Length** drop-down menu.

### Capacity Overview Dashboard

The Capacity Overview dashboard provides an overview of the capacity of the data centers in the environment. You can navigate between the data centers and review the status of the objects to see if you must rebalance the resource capacity among the data centers.

You can use the dashboard widgets in several ways.

- **Select an Environment:** Use this widget to select a data center. You can use the filter to narrow your list based on several parameters. After you identify the data center you want to view, select it. The dashboard is populated with the relevant data.
- **Total Capacity:** Use this widget to view the total physical capacity of the environment that includes capacity assigned as High Availability (HA). The actual capacity is less than the total capacity displayed when you consider HA and a buffer.
- **Reclaimable Capacity:** Use this widget to understand the amount of resources that can be freed up by deleting the powered off VMs. You can reclaim capacity from idle VMs, active VMs, orphaned VMs, and non-VMs. However, this widget highlights the capacity you can claim from powered off VMs. Powered off machines are VMs that are in a powered off state for a minimum percentage in the observation period. The default minimum percentage is 90% in the last 30 days. You can change this setting in the policy.
- **Memory Capacity Utilization Trend:** Use this widget to view the overall memory capacity trend. This widget displays the total physical resources you have. The physical resources include a HA buffer and a utilization buffer. This widget also displays the total memory you have allocated to VMs. If the number is close to the total physical capacity, the VMs may contend for memory. Ensure that the contention level is lower than what you promise to your customers. The chart also includes the actual utilization of memory capacity. The actual utilization is based on the active memory and hence it tends to be lower, as VMs do not normally access most of their RAM at any given moment.

- **CPU Capacity Utilization Trend:** Use this widget to view the overall CPU capacity trend. This widget displays the total physical resources you have. The physical resources include a HA buffer and a utilization buffer, which reflects the total capacity. This widget also displays the total CPU capacity you have allocated to VMs. If the number is close to the total physical capacity, the VMs may contend for CPU. Ensure that the contention level is lower than what you promise to your customers. The chart also includes the actual utilization of CPU. The actual utilization is based on the CPU demand counter, which takes into account the CPU used to perform I/O on behalf of the VM. The ESXi host performs storage I/O and network I/O on behalf of the VM, and this may be performed on a core that is different from the one on which the VM runs. As a result, CPU demand is a more accurate reflection of the VM CPU usage.
- **Disk Space Capacity Utilization Trend:** Use this widget to view the amount of disk space allocated to a VM and the amount that is actually used. This information is helpful when you plan for thin provisioning.
- **Capacity Utilization Distribution - What is Over or Under Utilized:** Use this widget to view if the objects in the data center are overused or underused. You can then carry out suitable actions on objects that are over used.

### Troubleshoot a VM Dashboard

Use the Troubleshoot a VM dashboard to troubleshoot performance problems of a single VM.

You can use the dashboard widgets in several ways.

- **Search for a VM to Troubleshoot:** Use this widget to view all the VMs in the environment. You can select the VM you want to troubleshoot. You can use the filter to narrow your list based on several parameters, such as name, folder name, associated tag, host, or vCenter Server. After you identify the VM you want to troubleshoot, select it. The dashboard is automatically populated with the relevant data.
- **About the VM:** Use this widget to understand the context of the VM. This widget also lends insights to analyze the root cause of the problem or potential mitigations.
- **Are there Critical Alerts:** Use this widget to view critical alerts. To see noncritical alerts, click the VM object.
- **Related Objects:** Use this widget to view the ESXi host where the VM is now running. This host might not be the ESXi host where the VM was running in the past. You can view the remaining related objects and see whether they might contribute to the problem.
- **Is the VMs Demand Spiking or Anomalous:** Use this widget to identify spikes in the VM demand for any of the resources such as CPU, memory, and network. Spikes in the demand might indicate an abnormal behavior of the VM or that the VM is undersized. The memory utilization is based on the Guest OS metric. It requires VMware Tools 10.0.0 or later and vSphere 6 Update 1 or later. If you do not have these products, the metric remains blank.
- **Is the VM Facing Contention:** Use this widget to identify whether the VM is facing contention. If the VM is facing contention, the underlying infrastructure might not have enough resources to meet the needs of the VM.

- **Does the Parent Cluster have Contention:** Use this widget to view the trend for the maximum CPU contention for a VM within the cluster. The trend might indicate a constant contention within the cluster. If there is contention, you must troubleshoot the cluster as the problem is no longer with the VM.
- **Does the Parent Datastore have Latency:** Use this widget to help you correlate the latency at the datastore level with the total latency of the VM. If the VM has latency spikes, but the datastore does not have such spikes, it might indicate a problem with the VM. If the datastore faces latency as well, you can troubleshoot to find out why the datastore has these spikes.
- **Parent Host and Parent Cluster:** Use these widgets to view the host and the cluster on which the VM resides.

## VM Dashboards

The VM Dashboards are a set of dashboards that provide insight into the configuration and behavior of VMs.

### Heavy Hitter VMs

The Heavy Hitter VMs dashboard provides information about the VMs that generated the highest IOPS and network throughput during the last week for a given cluster.

You can use the dashboard widgets in several ways.

- **Select a Cluster:** Use this widget to select a cluster. You can use the filter to narrow your list based on several parameters. After you identify the cluster you want to view, select it. The dashboard is automatically populated with the relevant data.
- **Cluster IOPS and Cluster Network Throughput:** Use these widgets to view the IOPS and network throughput for the cluster.
- Use the other widgets in the dashboard to view which VMs in the cluster generated the highest network throughput and IOPS. You can compare the information for the VM with the results for the cluster and correlate the trends. You can manually set the time to the time period for which you want to view data.

### VM Configuration Dashboard

The VM Configuration dashboard highlights the list of VMs with anomalous configuration. You can view VMs which have large snapshots that can be deleted. You can also view a list of orphaned VMs in the environment that can be deleted.

You can use the dashboard widgets in several ways.

- Use the Large VMs widgets to view graphical representations of VMs that have a large CPU, RAM, and disk space.
- View the VMs with limits, large snapshots, orphaned VMs, VMs with more than one NIC, and VMs with a nonstandard operating system. These VMs have a performance impact on the rest of the VMs in your environment even though they do not fully use their allocated resources.

You can customize the views in the widgets.

- 1 Click the **Edit Widget** icon from title bar of the widget. The **Edit** widget dialog box is displayed.

- 2 From the **Views** section, click the **Edit View** icon. The **Edit View** dialog box is displayed.
- 3 Click the **Presentation** option in the left pane and make the required modifications.

### VM Usage Dashboard

The VM Usage dashboard can be shared with the owner of the VM to help identify potential problems with the VM. It captures basic data about the VM. As there is no infrastructure-related data that is displayed in this dashboard, you can share the data in this dashboard with other teams without sharing infrastructure-related metrics.

You can use the dashboard widgets in several ways.

- **Search for a VM to Report its Usage:** Use this widget to select the VM you want to troubleshoot. You can use the filter to narrow your list based on several parameters. After you identify the VM that you want to view, select it. The dashboard is automatically populated with the relevant data.
- **About the VM:** Use this widget to view the VM you selected and its details. You select the VM in the Search for a VM to Report its Usage widget.
- **VM Utilization Trend: CPU, Memory, IOPS, Network:** Use this widget to view information about the usage and allocation trends for CPU demand, memory workload, disk commands per second, and the network usage rate.

### Infrastructure Dashboards

The Infrastructure Dashboards are a set of dashboards that provide insight into the configuration of clusters, datastores, and ESXi hosts.

#### Cluster Configuration Dashboard

The Cluster Configuration dashboard displays inconsistencies in any of the clusters in your environment.

You can use the dashboard widgets in several ways.

- **Is vMotion Configured Among All Hosts:** Use this widget to determine whether an inconsistency exists between the vMotion and HA configurations in the cluster. All ESXi hosts in a cluster should have consistent configuration. Consistent configuration of clusters makes operation easier and performance predictable.
- **Host Count across Clusters:** Use this widget to view all the clusters in your environment. If the clusters have a consistent number of hosts, the boxes displayed are of equal size. This representation helps you determine whether there is a large deviation among cluster sizes, whether there is a small cluster with fewer than four hosts, or whether there is a large cluster. Operationally, keep your clusters consistent and of moderate size.
- **Attributes of ESXi Hosts in the Selected Cluster:** Use this widget to view the configuration details for the hosts within a cluster.
- **All Clusters Properties:** Use this widget to view the properties for all the clusters in the widget.

#### Cluster Performance Dashboard

The Cluster Performance dashboard allows you to identify which clusters have VMs that suffer from memory contention and CPU contention.

You can use the dashboard widgets in several ways.

- **Clusters:** Use this widget to select the cluster for which you want to view performance details. You can use the filter to narrow your list based on several parameters. After you identify the cluster you want to view, select it. The dashboard is automatically populated with the relevant data.
- **Clusters Colored by Critical Alerts and Sized by Host Count:** Use this widget to view only the critical alerts.
- View the maximum and average CPU, memory disk, and disk latency for the VMs. If the VM faces contention, it might mean that the underlying infrastructure does not have enough resources to meet the needs of the VMs.
- View a list of 10 VMs that face CPU, memory, and disk latency contention. You can then troubleshoot and take steps to resolve the problem.

### Datastore Capacity Dashboard

The Datastore Capacity dashboard provides information that helps you understand whether you must rebalance the capacity of the datastores in the environment.

You can use the dashboard widgets in several ways.

- **Datastore Size and Usage Distribution:** Use this widget to find out which datastores are overused and which ones are underused. You can also find out whether the datastores are of equal size. When you select a datastore from this widget, the dashboard is automatically populated with the relevant data.
- **VMs in the Selected Datastore:** Use this widget to view a list of VMs based on the datastore you select. You can also view relevant details such as whether the VMs are powered on and the size of the snapshot if any.
- **Usage Trend of Selected Datastore:** Use this widget to find out the trends in capacity used by a selected datastore as against the total capacity available.
- **All Shared Datastores in the Environment:** Use this widget to view a list of datastores that are shared in your environment. The information displayed in this widget helps you make an informed decision about whether you have to rebalance the capacity of the datastores based on usage.

### Datastore Performance Dashboard

The Datastore Performance dashboard displays the datastores that have high latency and their corresponding trend line.

You can use the dashboard widgets in several ways.

- **Select a Datastore:** Use this widget to select the datastore for which you want to view performance details. You can use the filter to narrow your list based on several parameters. After you identify the datastore you want to view, select it. The dashboard is automatically populated with the relevant data.
- **Current IOPS and Latency of the VMs in the selected Datastore:** Use this widget to view the current IOPS and latency of the VMs in the selected datastore.

- **Datstores with High Latency and Outstanding IOs:** Use this widget to view those datstores with high latency and outstanding disk I/O trends. Ideally, your datstores must not have outstanding disk I/O.
- Use the other widgets in the dashboard to view trends for the selected datastore regarding disk latency, outstanding disk I/O, IOPS, and throughput.
- **Historical IOPS Trend of the selected VM** widget and the **Historical Latency Trend of the selected VM** widget: Use these widgets to view the historical trend of IOPS and latency for a VM in the selected datastore. From the Current IOPS and Latency of the VMs in the selected Datastore widget, select a VM to populate the historical trends.

### ESXi Configuration Dashboard

The ESXi Configuration dashboard provides configuration and distribution information of the ESXi hosts in your environment. You can also find out whether any of the hosts are configured with non-recommended settings.

You can use the dashboard widgets in several ways.

- Use the widgets to determine the distribution of hardware models, BIOS versions, and ESXi versions in your environment.
- Use the widgets to determine whether any of the hosts are configured with non-recommended settings that include ESXi hosts in a disconnected state, ESXi hosts in maintenance mode, and hosts with a network speed that is below 10 GB.
- **All ESXi Configuration:** Use this widget to identify a mismatch in the host configuration.

### Network Configuration Dashboard

The Network Configuration dashboard helps you find out which ESXi hosts and VMs use a specific switch.

You can use the dashboard widgets in several ways.

- **Distributed Switches:** Use this widget to select the switch for which you want to view details. You can use the filter to narrow your list based on several parameters. After you identify the switch that you want to view, select it. The dashboard is automatically populated with the relevant data.
- **Distributed Port Groups on the Switch:** Use this widget to view the port groups on the switch, how many ports each switch has, and the usage details.
- **ESXi Hosts/VMs Using the Selected Switch:** Use these widgets to find out which ESXi hosts and VMs use the selected switch. You can also view configuration details about the ESXi hosts and VMs that use the selected switch.

### Custom Dashboards

vRealize Operations Manager has predefined dashboards. You can also create dashboards that meet your environment needs.

To manage your **Dashboards** and your vRealize Operations Manager home page, click the **Content** icon in the left pane and click **Dashboards**.

Depending on your access rights, you can add, delete, and arrange widgets on your dashboards, clone and create new dashboards, import or export dashboards from other instances, edit widget configuration options, and configure widget interactions.

**Table 6-4. Dashboards Options**

Option	Description	Usage
Save as Template	Contains all the information in a dashboard definition.	You can use any dashboard to create a template.
Export Dashboard	When you export a dashboard, vRealize Operations Manager creates a dashboard file in JSON format.	You can export a dashboard from one vRealize Operations Manager instance and import it to another.
Import Dashboard	A JSON file that contains dashboard information from vRealize Operations Manager.	You can import a dashboard that was exported from another vRealize Operations Manager instance. You can import dashboards with XML files from vRealize Operations Manager 5.x instances.
Add Dashboard(s) to Home	Makes a dashboard available on the vRealize Operations Manager home page.	You can add any dashboard to the vRealize Operations Manager home page.
Remove Dashboard(s) from Home	Removes a dashboard from the vRealize Operations Manager home page.	You can add any dashboard to the vRealize Operations Manager home page.
Reorder/Autoswitch Dashboards	Changes the order of the dashboard tabs on vRealize Operations Manager home page.	You can configure vRealize Operations Manager to switch from one dashboard to another.
Manage Summary Dashboards	Provides you with an overview of the state of the selected object, group, or application.	You can change the <b>Summary</b> tab with a dashboard to get information specific to your needs.
Manage Tab Groups	Groups dashboards in folders.	You can create dashboard folders to group the dashboards in a way that is meaningful to you.
Share Dashboards	Makes a dashboard available to other users or user groups.	You can share a dashboard or dashboard template with one or more user groups.

The dashboard list depends on your access rights.

## Create and Configure Dashboards

To view the status of all objects in vRealize Operations Manager, create a dashboard by adding widgets. You can create and modify dashboards and configure them to meet your environment needs.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Dashboards**.
- 2 Click the **Create Dashboard** icon to create and configure a dashboard.

3 Complete the steps in the left pane to:

- a Enter a name for the dashboard.

[Name and Description Details](#)

- b Add widgets to the dashboard.

[Widget List Details](#)

- c Configure widget interactions.

[Widget Interactions Details](#)

- d Create dashboard navigation.

[Dashboard Navigation Details](#)

4 Click **Save**.

5 From the Dashboards panel, click **Edit Dashboard** to modify the dashboard.

## Name and Description Details

The name and visualization of the dashboard as it appears on the vRealize Operations Manager Home page.

### Where You Configure a Dashboard

To create or edit your dashboard, select **Content > Dashboards** in the left pane. On the Dashboards toolbar, click the plus sign to add a dashboard or the pencil to edit the selected dashboard. In the workspace, on the left, click **Dashboard Configuration**.

**Table 6-5. Dashboard Configuration Options in the Dashboard Workspace**

Option	Description
Name	Name of the dashboard as it appears on top of the tab on the Home page and in the dashboard's lists.  If you use a forward slash while entering a name, the forward slash acts as a group divider and creates a folder with the specified name in the dashboards list if the name does not exist. For example, if you name a dashboard <b>clusters/hosts</b> , the dashboard is named hosts under the group clusters.
Description	Description of the dashboard.
Is default	If you select <b>Yes</b> , the dashboard appears on the Home page when you log in.

## Widget List Details

vRealize Operations Manager provides a list of widgets that you can add to your dashboard to monitor specific metrics and properties of objects in your environment.

## Where You Add Widgets to a Dashboard

To add a widget to your dashboard, select **Content > Dashboards** in the left pane. On the Dashboards toolbar, click the plus sign to add a dashboard or the pencil icon to edit the selected dashboard. In the workspace, on the left, click **Widget List**. If you create a dashboard, complete the required previous steps of the workspace.

## How to Add Widgets to a Dashboard

In the workspace, on the left, you see a list with all the predefined vRealize Operations Manager widgets. To add a widget to the dashboard, drag the widget to the content area on the right.

To locate a widget, you can type the name or part of the name of a widget in the **Filter** option. For example, when you enter **cap**, the list is filtered to display the Capacity Remaining, Capacity Utilisation, and Reclaimable Capacity widgets. You can then select the widget you require.

Most widgets must be configured individually to display information. For more information about how to configure each widget, see [Widgets](#).

## How to Arrange Widgets in a Dashboard

You can modify your dashboard layout to suit your needs. By default, the first widgets that you add are automatically arranged horizontally wherever you place them. The widgets move up to the highest position in the dashboard based on their width.

- To position a widget, drag the widget to the desired location in the layout. Other widgets automatically rearrange to make room.
- To resize a widget, drag the bottom right corner of the widget.

## Widget Interactions Details

You can connect widgets so that the information they show depends on each other.

## Where You Create Widget Interactions

To create a widget interaction for widgets in a dashboard, select **Content > Dashboards** in the left pane. On the Dashboards toolbar, click the plus sign to add a dashboard or the pencil to edit the selected dashboard. In the workspace, on the left, click **Widget Interactions**. If you create a new dashboard, complete the required previous steps of the workspace.

## How to Create Widget Interactions

The list of available widget interactions depends on the widgets in the dashboard. Widgets can provide, receive, and do both. Some widgets can have more than one provider.

To create interactions, click the **Selected Object(s)** drop-down menu for the specified widget and select the provider widget. There are widgets that provide alerts, metrics, or tags. Click the **Selected Alert(s)**, **Selected Metric(s)**, or **Selected Tag(s)** drop-down menu to select the alert, metric, or tag specific provider widget. When you are ready with all interactions, click **Apply Interactions**. For more information about how interactions work, see [Widget Interactions](#).

## Dashboard Navigation Details

You can use dashboard navigation to move from one dashboard to another, and to apply sections or context from one dashboard to another. You can connect a widget to widgets on other dashboards to investigate problems or better analyze the provided information.

### Where You Add Dashboard Navigation

To create a dashboard navigation to a dashboard, select **Content > Dashboards** in the left pane. On the Dashboards toolbar, click the plus sign to add a dashboard or the pencil to edit the selected dashboard. In the workspace, on the left, click **Dashboard Navigation**. If you create a new dashboard, complete the required previous steps of the workspace.

### How Dashboard Navigation Works

You can create dashboard navigation only for provider widgets. The provider widget sends information to the destination widget. When you create dashboard navigation, the destination widgets are filtered based on the information type they can receive.

### How to Add a Dashboard Navigation to a Dashboard

The list of available dashboard navigations depends on the available dashboards and the widgets in the current dashboard. To add navigation, click the **Destination Dashboards** drop-down menu for the specified widget and select the dashboard and the widget to navigate to. You can select more than one applicable widget. Click **Apply Navigations** to apply the connections.

---

**Note** If a dashboard is unavailable at the Home page, it is unavailable for dashboard navigation.

---

The Dashboard Navigation icon () appears in the top menu of each widget when a dashboard navigation is available. You can select multiple objects to apply selections or context from one dashboard to another. Press Ctrl+click to select multiple individual objects or Shift+click to select a range of objects.

## Managing Dashboards

You can change the order of the dashboard tabs, configure vRealize Operations Manager to switch from one dashboard to another, create dashboard folders to group the dashboards in a way that is meaningful to you, and share a dashboard or dashboard template with one or more user groups.

### Reorder and Switch Dashboards

You can change the order of the dashboard tabs on your home page. You can configure vRealize Operations Manager to switch from one dashboard to another. This feature is useful if you have several dashboards that show different aspects of your enterprise's performance and you want to look at each dashboard in turn.

### Where You Configure a Dashboard Order and Automatic Switch

To reorder and configure a dashboard switch, select **Content > Dashboards** in the left pane, click the gear icon and select **Reorder/Autoswitch Dashboards**.

## How You Reorder the Dashboards

The list shows the dashboards as they are ordered. Drag the dashboards up and down to change their order on the home page.

## How You Configure an Automatic Dashboard Switch

- 1 Double click a dashboard from the list to configure.
- 2 From the Auto Transition drop-down menus, select **On**.
- 3 Select the switch time interval in seconds.
- 4 Select the dashboard to switch to and click **Update**.
- 5 Click **Save** to save your changes.

On the home page, the current dashboard will switch to the dashboard that is defined after the specified time interval.

## Manage Summary Dashboards

The **Summary** tab provides you with an overview of the state of the selected object, group, or application. You can change the **Summary** tab with a dashboard to get information specific to your needs.

### Where You Configure a Summary Tab Dashboard

To manage the summary dashboards, select **Content > Dashboards** in the left pane, click the gear icon and select **Manage Summary Dashboards**.

### How You Manage the Summary Tab Dashboard

**Table 6-6. Manage Summary Dashboards Options**

Option	Description
Adapter Type	Adapter type for which you configure a summary dashboard.
Filter	Use a word search to limit the number of adapter types that appear in the list.
Name	List with all available objects.
Use Default icon	Click to use vRealize Operations Manager default <b>Summary</b> tab.
Detail Page	Shows what kind of <b>Summary</b> tab you use for the selected object.
Assign a Dashboard icon	Click to view the Dashboard List dialog box that lists all the available dashboards.

To change the Summary tab for an object, select the object in the left panel, click the **Assign a Dashboard** icon. Select a dashboard for it from the Dashboard List dialog box and click **OK**. From the Manage Summary Dashboards dialog box click **Save**. You will see the dashboard you have associated to the object type when you navigate to the **Summary** tab of the object details page.

## Manage Tab Groups

You can create dashboard folders to group the dashboards in a way that is meaningful to you.

### Where You Configure a Dashboard Group

To manage the dashboard groups, select **Content > Dashboards** in the left pane, click the gear icon and select **Manage Tab Groups**.

### How You Manage the Dashboard Tabs

**Table 6-7. Manage Tap Groups Options**

Option	Description
Tab Groups	A hierarchy tree with all available group folders.
Dashboard Tabs	A list with all available dashboards.

To create a new dashboard group folder, right-click the **Tab Groups** folder or another folder and click **Add**. To add a dashboard, drag one from the Dashboard Tabs list to the folder.

## Share Dashboards

You can share a dashboard or dashboard template with one or more user groups. When you share a dashboard, it becomes available to all of the users in the user group that you select. The dashboard appears the same to all of the users who share it. If you edit a shared dashboard, the dashboard changes for all users. Other users can only view a shared dashboard. They cannot change it.

### Where You Share a Dashboard From

To share a dashboard, select **Content > Dashboards** in the left pane, click the gear icon and select **Share Dashboards**.

**Table 6-8. Share Dashboards Options**

Option	Description
Accounts Group	All available groups with which you can share a dashboard.
Shared Dashboards	All available dashboards and templates that you can share. You can switch between dashboard tabs and dashboard templates by clicking the <b>Share Dashboard Tab/Template</b> icon.

### How You Manage a Shared Dashboard Tab

To share a dashboard tab, navigate to the dashboard in the list of Shared Dashboards and drag it to the group to share it with on the left.

To stop sharing a dashboard with a group, click that group on the left panel, navigate to the dashboard in the right panel, and click the **Stop Sharing** icon above the list.

To stop sharing a dashboard with more than one group, click the **Not Grouped** name on the left panel, navigate to the dashboard in the right panel, and click the **Stop Sharing** icon above the list.

## Views

vRealize Operations Manager provides several types of views. Each type of view helps you to interpret metrics, properties, policies of various monitored objects including alerts, symptoms, and so on, from a different perspective. vRealize Operations Manager Views also show information that the adapters in your environment provide.

You can configure vRealize Operations Manager views to show transformation, forecast, and trend calculations.

- The transformation type determines how the values are aggregated.
- The trend option shows how the values tend to change, based on the historical, raw data. The trend calculations depend on the transformation type and roll up interval.
- The forecast option shows what the future values can be, based on the trend calculations of the historical data.



Create Views

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_create\\_views\\_in\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_create_views_in_vrom))

You can use vRealize Operations Manager views in different areas of vRealize Operations Manager.

- To manage all views, select **Content > Views**.
- To see the data that a view provides for a specific object, navigate to that object, click the **Details** tab, and click **Views**.
- To see the data that a view provides in your dashboard, add the View widget to the dashboard.
- To have a link to a view in the Further Analysis section, select the Further Analysis option on the view workspace visibility step.

## Views and Reports Ownership

The default owner of all predefined views and templates is System. If you edit them, you become the owner. If you want to keep the original predefined view or template, you have to clone it. After you clone it, you become the owner of the clone.

The last user who edited a view, template, or schedule is the owner. For example, if you create a view you are listed as its owner. If another user edits your view, that user becomes the owner listed in the Owner column.

The user who imports the view or template is its owner, even if the view is initially created by someone else. For example, *User 1* creates a template and exports it. *User 2* imports it in back, the owner of the template becomes *User 2*.

The user who generated the report is its owner, regardless of who owns the template. If a report is generated from a schedule, the user who created the schedule is the owner of the generated report. For example, if *User 1* creates a template and *User 2* creates a schedule for this template, the generated report owner is *User 2*.

## Views Overview

A view presents collected information for an object in a certain way depending on the view type. Each type of view helps you to interpret metrics, properties, policies of various monitored objects including alerts, symptoms, and so on, from a different perspective.

The Views page is available when you click the **Content** icon in the left pane and click **Views**.

On the Views page you can create, edit, delete, clone, export, and import views.

You can order the listed views by name, type, description, subject, or owner.

You can limit the views list by adding a filter from the upper-right corner of the panel.

**Table 6-9. Filter Groups**

Filter Group	Description
Name	Filter by the view name. For example, type <b>my view</b> to list all views that contain the my view phrase in their name.
Type	Filter by the view type.
Description	Filter by the view description. For example, type <b>my view</b> to list all views that contain the my view phrase in their description.
Subject	Filter by the subject.

## Views and Reports Ownership

Views, reports, templates, or schedules owner might change in time.

The default owner of all predefined views and templates is System. If you edit them, you become the owner. If you want to keep the original predefined view or template, you have to clone it. After you clone it, you become the owner of the clone.

The last user who edited a view, template, or schedule is the owner. For example, if you create a view you are listed as its owner. If another user edits your view, that user becomes the owner listed in the Owner column.

The user who imports the view or template is its owner, even if the view is initially created by someone else. For example, *User 1* creates a template and exports it. *User 2* imports it in back, the owner of the template becomes *User 2*.

The user who generated the report is its owner, regardless of who owns the template. If a report is generated from a schedule, the user who created the schedule is the owner of the generated report. For example, if *User 1* creates a template and *User 2* creates a schedule for this template, the generated report owner is *User 2*.

## Create and Configure a View

To collect and display information for a specific object, you can create a custom view.

## Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Views**.
- 2 Click the **Create View** icon to create a view.
- 3 Complete the steps in the left pane to:
  - a Enter a name and description for the view.  
[Name and Description Details](#)
  - b Change the presentation of a view.  
[Presentation Details](#)
  - c Select the base object type for a view.  
[Subjects Details](#)
  - d Add data to a view.  
[Data Details](#)
  - e Change the visibility of a view.  
[Visibility Details](#)
- 4 Click **Save**.
- 5 From the Dashboards panel, click **Edit View** to modify the view.

## Name and Description Details

The name and description of the view as they appear in the list of views on the Views page.

To add a name and description to a view, select **Content > Views** in the left pane. On the Views toolbar, click the plus sign to add a view or the pencil to edit the selected view. In the workspace, on the left, click **Name and Description**.

**Table 6-10. Name and Description Options in the View Workspace**

Option	Description
Name	Name of the view as it appears on the Views page.
Description	Description of the view.

## Presentation Details

A presentation is a way the collected information for the object is presented. Each type of view helps you to interpret metrics and properties from a different perspective.

To change the presentation of a view, select **Content > Views** in the left pane. On the Views toolbar, click the plus sign to add a view or the pencil to edit the selected view. In the workspace, on the left, click **Presentation**. If you create a view, complete the required previous steps.

**Table 6-11. Presentation Options in the View Workspace**

View Type	Description
List	Provides tabular data about specific objects in the monitored environment.
Summary	Provides tabular data about the use of resources in the monitored environment.
Trend	Uses historic data to generate trends and forecasts for resource use and availability in the monitored environment.
Distribution	Provides aggregated data about resource distribution in the monitored environment.
Text	<p>Inserts the provided text. The text can be dynamic and contain metrics and properties.</p> <p>You can format text to increase or decrease the font size, change the font color, highlight text, and align text to the left, right, or center. You can also make the selected text appear bold, in italics, or underlined.</p> <p>By default the text view is available only for report template creation and modification. You can change this on the <b>Visibility</b> step of the view workspace.</p>
Image	<p>Inserts a static image.</p> <p>By default the image view is available only for report template creation and modification. You can change this on the <b>Visibility</b> step of the view workspace.</p>

You can see a live preview of the view type when you select a subject and data, and **Select preview source**.

### How to Configure the Presentation of a View

Some of the view presentations have specific configuration settings.

**Table 6-12. Presentation Configuration Options in the View Workspace**

View Type	Configuration Description
List	Select the number of items per page. Each item is one row and its metrics and properties are the columns.
Summary	Select the number of items per page. Each row is an aggregated metric or property.

View Type	Configuration Description
Trend	<p>Enter the maximum number of plot lines. Limits the output in terms of the objects displayed in the live preview of the view type on the left upper pane. The number you set as the maximum number of plot lines determines the plot lines.</p> <p>For example, if you plot historical data and set the maximum at 30 plot lines, then 30 objects are displayed. If you plot historical, trend, and forecast lines, and set the maximum to 30 plot lines, then only 10 objects are displayed as each object has three plot lines.</p>
Distribution	<p>Select the visualization of the distribution information in a pie chart or a bar chart.</p> <p>Select the distribution type, and configure the buckets count and size.</p> <p>To understand vRealize Operations Manager distribution type, see <a href="#">View Distribution Type</a>.</p>

## Distribution Type

vRealize Operations Manager view distribution type provides aggregated data about resource distribution in the monitored environment.

**Dynamic distribution** You specify in details how vRealize Operations Manager distributes the data in the buckets.

**Table 6-13. Dynamic Distribution Configuration Options**

Configuration Option	Description
Buckets Count	The number of buckets to use in the data distribution.
Buckets Size Interval	The bucket size is determined by the defined interval divided by the specified number of buckets.
Buckets Size Logarithmic bucketing	The bucket size is calculated to logarithmically increasing sizes. This provides a continuous coverage of the whole range with the specified number of buckets. The base of the logarithmic sizing is determined by the given data.
Buckets Size Simple Max/Min bucketing	The bucket size is divided equally between the measured min and max values. This provides a continuous coverage of the whole range with the specified number of buckets.

**Manual distribution** You specify the number of buckets and the minimum and maximum values of each bucket.

**Discrete distribution** You specify the number of buckets in which vRealize Operations Manager distribute the data.

## View Distribution Type

vRealize Operations Manager view distribution type provides aggregated data about resource distribution in the monitored environment.

**Dynamic distribution** You specify in details how vRealize Operations Manager distributes the data in the buckets.

**Table 6-14. Dynamic Distribution Configuration Options**

Configuration Option	Description
Buckets Count	The number of buckets to use in the data distribution.
Buckets Size Interval	The bucket size is determined by the defined interval divided by the specified number of buckets.
Buckets Size Logarithmic bucketing	The bucket size is calculated to logarithmically increasing sizes. This provides a continuous coverage of the whole range with the specified number of buckets. The base of the logarithmic sizing is determined by the given data.
Buckets Size Simple Max/Min bucketing	The bucket size is divided equally between the measured min and max values. This provides a continuous coverage of the whole range with the specified number of buckets.

**Manual distribution** You specify the number of buckets and the minimum and maximum values of each bucket.

**Discrete distribution** You specify the number of buckets in which vRealize Operations Manager distribute the data.

If you increase the number of buckets, you can see more detailed data.

## Subjects Details

The subject is the base object type for which the view shows information.

To specify a subject for a view, select **Content > Views** in the left pane. On the Views toolbar, click the plus sign to add a view or the pencil to edit the selected view. In the workspace, on the left, click **Subjects**. If you create a new view, complete the required previous steps.

The subject you specify determines where the view is applicable. If you select more than one subject, the view is applicable for each of them. You can limit the level where the view appears with the Blacklist option in the **Visibility** step.

View availability depends on the view configuration subject, inventory view, user permissions, and view Visibility settings.

## Views Applicability

### List View

When you navigate through the environment tree, you can see the List view at the subjects that you specify during the view configuration and at their object containers. Depending on the inventory view, the List view might be missing at the object containers. For example, you create a List view with subject Host System. When you go to **Environment > vSphere Hosts and Clusters > vSphere World**, select a vCenter Server, and click the **Details** tab, you can see your List view. If you go to **Environment > vSphere Storage > vSphere World**, select the same vCenter Server, and click the **Details** tab, your List view is missing. Your List view with subject Host System is missing because the object Host System is not included in the vSphere Storage inventory view.

### Summary View

When you navigate through the environment tree, you can see the Summary view at the subjects that you specify during the view configuration and at their object containers. Depending on the inventory view, the Summary view might be missing at the object containers. For example, you create a Summary view with subject Datastore. When you go to **Environment > vSphere Storage > vSphere World**, select a vCenter Server, and click the **Details** tab, you can see your List view. If you go to **Environment > vSphere Networking > vSphere World**, select the same vCenter Server, and click the **Details** tab, your Summary view is missing. Your Summary view with subject datastore is missing because the object Datastore is not included in the vSphere Networking inventory view.

### Trend View

When you navigate through the environment tree, you can see the Trend view only at the subjects that you specify during the view configuration. For example, you create a Trend view with subject Virtual Machine. When you navigate to a virtual machine in the navigation tree, you see your view.

### Distribution View

When you navigate through the environment tree, you can see the Distribution view only at the object containers of the subjects that you specify during the view configuration. Depending on the inventory view, the Distribution view might be missing at the object containers. For example, you create a Distribution view with subject Host System. When you go to **Environment > vSphere Hosts and Clusters > vSphere World**, select a vCenter Server, and click the **Details** tab, you can see your Distribution view. If you go to **Environment > vSphere Networking > vSphere World**, select the same vCenter Server, and click the **Details** tab, your Distribution view is missing. Your Distribution view with subject Host System is missing because the object Host System is not included in the vSphere Networking inventory view.

### Text View

When you navigate through the environment tree, you can see the Text view only at the subjects that you specify during the view configuration. For

example, you create a Text view with subject vCenter Server. When you navigate to a vCenter Server in the navigation tree, you see your view. If you did not specify a subject, you see your view for every subject in the environment.

**Image View** The Image view is applicable for every object in the environment.

---

**Note** Views applicability depends also on your user permissions and the view Visibility configuration.

---

### Views Applicability

Views might not always appear where you expect them to. The main applicability of views depends on the view subject and the inventory view.

**List View** When you navigate through the environment tree, you can see the List view at the subjects that you specify during the view configuration and at their object containers. Depending on the inventory view, the List view might be missing at the object containers. For example, you create a List view with subject Host System. When you go to **Environment > vSphere Hosts and Clusters > vSphere World**, select a vCenter Server, and click the **Details** tab, you can see your List view. If you go to **Environment > vSphere Storage > vSphere World**, select the same vCenter Server, and click the **Details** tab, your List view is missing. Your List view with subject Host System is missing because the object Host System is not included in the vSphere Storage inventory view.

**Summary View** When you navigate through the environment tree, you can see the Summary view at the subjects that you specify during the view configuration and at their object containers. Depending on the inventory view, the Summary view might be missing at the object containers. For example, you create a Summary view with subject Datastore. When you go to **Environment > vSphere Storage > vSphere World**, select a vCenter Server, and click the **Details** tab, you can see your List view. If you go to **Environment > vSphere Networking > vSphere World**, select the same vCenter Server, and click the **Details** tab, your Summary view is missing. Your Summary view with subject datastore is missing because the object Datastore is not included in the vSphere Networking inventory view.

**Trend View** When you navigate through the environment tree, you can see the Trend view only at the subjects that you specify during the view configuration. For example, you create a Trend view with subject Virtual Machine. When you navigate to a virtual machine in the navigation tree, you see your view.

**Distribution View** When you navigate through the environment tree, you can see the Distribution view only at the object containers of the subjects that you specify during the view configuration. Depending on the inventory view, the Distribution view might be missing at the object containers. For example,

you create a Distribution view with subject Host System. When you go to **Environment > vSphere Hosts and Clusters > vSphere World**, select a vCenter Server, and click the **Details** tab, you can see your Distribution view. If you go to **Environment > vSphere Networking > vSphere World**, select the same vCenter Server, and click the **Details** tab, your Distribution view is missing. Your Distribution view with subject Host System is missing because the object Host System is not included in the vSphere Networking inventory view.

### Text View

When you navigate through the environment tree, you can see the Text view only at the subjects that you specify during the view configuration. For example, you create a Text view with subject vCenter Server. When you navigate to a vCenter Server in the navigation tree, you see your view. If you did not specify a subject, you see your view for every subject in the environment.

### Image View

The Image view is applicable for every object in the environment.

---

**Note** Views applicability depends also on your user permissions and the view Visibility configuration.

---

## Data Details

The data definition process includes adding properties, metrics, policies, or data that adapters provide to a view. These are the items by which vRealize Operations Manager collects, calculates, and presents the information for the view.

To add data to a view, select **Content > Views** in the left pane. On the Views toolbar, click the plus sign to add a view or the pencil to edit the selected view. In the workspace, on the left, click **Data**. If you create a new view, complete the required previous steps.

### How to Add Data to a View

If you selected more than one subject, specify the subject for which you add data. Double-click the data from the tree in the left panel to add it to the view. For each subject the data available to add might be different.

### How to Configure the Data Transformation

The data configuration options depend on the view and data type that you select. Most of the options are available for all views.

**Table 6-15. Data Configuration Options**

Configuration Option	Description
Metric name	Default metric name. Available for all views.
Metric label	Customizable label as it appears in the view or report. Available for all views.

Configuration Option	Description
Units	<p>Depends on the added metric or property. You can select in what unit to display the values. For example, for CPU  Demand(MHz) from the <b>Units</b> drop-down menu, you can change the value to Hz, KHz, or GHz. If you select <b>Auto</b>, the scaling is set to a meaningful unit.</p> <p>Available for all views.</p>
Sort order	<p>Orders the values in ascending or descending order.</p> <p>Available for List view and Summary view.</p>
Transformation	<p>Determines what calculation method is applied on the raw data. You can select the type of transformation:</p> <ul style="list-style-type: none"> <li>■ Minimum. The minimum value of the metric over the selected time range.</li> <li>■ Maximum. The maximum value of the metric over the selected time range.</li> <li>■ Average. The mean of all the metric values over the selected time range.</li> <li>■ Sum. The sum of the metric values over the selected time range.</li> <li>■ Last. Ignores all the data except the data you receive most recently and that is within the selected time range.</li> <li>■ Standard Deviation. The standard deviation of the metric values.</li> <li>■ Metric Correlation. Displays the value when another metric is at the minimum or maximum. For example, displays the value for memory.usage when cpu.usage is at a maximum.</li> <li>■ Forecast. Performs a regressive analysis and predicts future values. Displays the last metric value of the selected range.</li> </ul> <p>Available for all views, except Trend.</p>
Data Series	<p>You can select whether to include historical data, trend of historical data, and forecast for future time in the trend view calculations.</p> <p>Available for Trend view.</p>
Series Roll up	<p>The time interval at which the data is rolled up. You can select one of the available options. For example, if you select <b>Sum</b> as a Transformation and 5 minutes as the roll-up interval, then the system selects 5-minute interval values and adds them.</p> <p>This option is applicable to the Transformation configuration option.</p> <p>Available for all views.</p>
Projects	<p>A project contains scenarios and is a supposition about how capacity and load change if certain conditions are changed without making actual changes to your virtual infrastructure. If you implement the project, you know in advance what your capacity requirements are.</p> <p>Available for all views. Depends on the selected metrics and properties.</p>

## How to Configure Time Settings

Use the time settings to select the time interval of data transformation. These options are available for all view types, except Image.

You can set a time range for a past period or set a future date for the end of the time period. When you select a future end date and no data is available, the view is populated by forecast data.

**Table 6-16. Time Settings Options**

Configuration Option	Description
Time Range Mode	In Basic mode you can select date ranges. In Advanced mode you can select any combination of relative or specific start and end dates.
Relative Date Range	Select a relative date range of data transformation. Available in Basic mode.
Specific Date Range	Select a specific date range of data transformation. Available in Basic mode.
Absolute Date Range	Select a date or time range to view data for a time unit such as a complete month or a week. For example, you can run a report on the third of every month for the previous month. Data from the first to the end of the previous month is displayed as against data from the third of the previous month to the third of the current month. The units of time available are: <b>Hours, Days, Weeks, Months, and Years</b> . The locale settings of the system determine the start and end of the unit. For example, weeks in most of the European countries begin on Monday while in the United States they begin on Sunday. Available in Basic mode.
Relative Start Date	Select a relative start date of data transformation. Available in Advanced mode.
Relative End Date	Select a relative end date of data transformation. Available in Advanced mode.
Specific Start Date	Select a specific start date of data transformation. Available in Advanced mode.
Specific End Date	Select a specific end date of data transformation. Available in Advanced mode.
Currently selected date range	Displays the date or time range you selected. For example, if you select a specific date range from 5/01/2016 to 5/18/2016, the following information is displayed: May 1, 2016 12:00:00 AM to May 18, 2016 11:55:00 PM.

## How to Break Down Data

You can break down data in List views by adding interval or instance breakdown columns from the **Group By** tab.

**Table 6-17. Group By Options**

Option	Description
Add interval breakdown column (see data for column settings)	<p>Select this option to see the data for the selected resources broken down in time intervals.</p> <p>In the <b>Data</b> tab, select <b>Interval Breakdown</b> to configure the column. You can enter a label and select a breakdown interval for the time range.</p>
Add instance breakdown column (see data for column settings)	<p>Select this option to see the data for all instances of the selected resources.</p> <p>In the <b>Data</b> tab, select <b>Instance Name</b> to configure the column. You can enter a label and select a metric group to break down all the instances in that group. Deselect <b>Show non-instance aggregate metric</b> to display only the separate instances. Deselect <b>Show only instance name</b> to display the metric group name and instance name in the instance breakdown column.</p> <p>For example, you can create a view to display CPU usage by selecting the metric <b>CPU:0 Usage</b>. If you add an instance breakdown column, the column CPU:0 Usage displays the usage of all CPU instances on separate rows (0, 1 and so on). To avoid ambiguity, you can change the metric label of <b>CPU:0 Usage</b> to <b>Usage</b>.</p>

### How to Add a Filter

The filter option allows you to add additional criteria when the view displays too much information. For example, a list view shows information about the health of virtual machines. From the **Filter** tab you add a risk metric less than 50%. Then the view will show the health of all virtual machines with risk less than 50%.

To add filter to a view, select **Content > Views** in the left pane. On the Views toolbar, click the plus sign to add a view or the pencil to edit the selected view. In the workspace, on the left, click **Data** and click the **Filter** tab in the main panel. If you create a new view, complete the required previous steps.

Each subject has a separate filter box. For Alerts Rollup, Alert, and Symptom subjects not all applicable metrics are supported for filtering.

**Table 6-18. Filter Add Options**

Option	Description
Add	Adds another criteria to the criteria set. The filter returns results that match all of the specified criteria.
Add another criteria	Adds another criteria set. The filter returns results that match one criteria set or another.

## How to Add a Summary Row or Column to a View

The summary option is available only for List and Summary views. It is mandatory for the Summary views. You can add more than one summary row or column and configure each to show different aggregations. In the summary configuration panel, you select the aggregation method and what data to include or exclude from the calculations.

To add a summary row or column to a view, select **Content > Views** in the left pane. On the Views toolbar, click the plus sign to add a view or the pencil to edit the selected view. In the workspace, on the left, click **Data** and click the **Summary** tab in the main panel. If you create a new view, complete the required previous steps.

For the List view, the summary row shows aggregated information by the specified subjects.

For the Summary view, the summary column shows aggregated information by the items provided on the **Data** tab.

## Visibility Details

The view visibility defines where you can see a view in vRealize Operations Manager.

To change the visibility of a view, select **Content > Views** in the left pane. On the Views toolbar, click the plus sign to add a view or the pencil to edit the selected view. In the workspace, on the left, click **Visibility**. If you create a new view, complete the required previous steps.

**Table 6-19. View Workspace Visibility Options**

Option	Description
Availability	Select where in vRealize Operations Manager you want to see this view. If you want to have the view available in a dashboard, select the check box, add the View widget, and configure it.
Further Analysis	Select a badge to make the view available at Further Analysis. Further Analysis section appears on the Analysis tab of an object. When you make a view visible for a badge, a link to it appears in the Further Analysis section of that badge. You can click on the link to analyse the provided information.
Blacklist	Select a subject level where you do not want to see this view. For example, you have a list view with subject virtual machines. It is visible when you select any of its parent objects. You add datacenter in the blacklist. The view is not visible anymore on datacenter level.

## Editing, Cloning, and Deleting a View

You can edit, clone, and delete a view. Before you do, familiarize yourself with the consequences of these actions.

When you edit a view, all changes are applied to the report templates that contain it.

When you clone a view, the changes that you make to the clone do not affect the source view.

When you delete a view, it is removed from all the report templates that contain it.

## User Scenario: Create, Run, Export, and Import a vRealize Operations Manager View for Tracking Virtual Machines

As a virtual infrastructure administrator, you use vRealize Operations Manager to monitor several environments. You must know the number of virtual machines on each vCenter Server instance. You define a view to gather the information in a specific order and use it on all vRealize Operations Manager environments.

### Prerequisites

Verify that you have the necessary access rights to perform this task. Your vRealize Operations Manager administrator can tell you which actions you can perform.

You will create a distribution view and run it on the main vRealize Operations Manager environment. You will export the view and import it in another vRealize Operations Manager instance.

### Procedure

#### 1 [Create a vRealize Operations Manager View for Supervising Virtual Machines](#)

To collect and display data about the number of virtual machines on a vCenter Server, you create a custom view.

#### 2 [Run a vRealize Operations Manager View](#)

To verify the view and capture a snapshot of information at any point, you run the view for a specific object.

#### 3 [Export a vRealize Operations Manager View](#)

To use a view in another vRealize Operations Manager, you export a content definition XML file.

#### 4 [Import a vRealize Operations Manager View](#)

To use views from other vRealize Operations Manager environments, you import a content definition XML file.

## Create a vRealize Operations Manager View for Supervising Virtual Machines

To collect and display data about the number of virtual machines on a vCenter Server, you create a custom view.

### Procedure

1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Views**.

2 Click the plus sign to create a new view.

3 Enter **Virtual Machines Distribution**, the name for the view.

4 Enter a meaningful description for the view.

For example, **A view showing the distribution of virtual machines per hosts.**

- 5 Click **Presentation** and select the **Distribution** view type.

The view type is the way the information is displayed.

- a From the **Visualization** drop-down menu, select **Pie Chart**.
- b From the Distribution Type configurations, select **Discrete distribution**.

Leave **Max number of buckets** deselected because you do not know the number of hosts on each vCenter Server instance. If you specify a number of buckets and the hosts are more than that number, one of the slices shows unspecified information labeled Others.

- 6 Click **Subjects** to select the object type that applies to the view.

- a From the drop-down menu, select **Host System**.

The Distribution view is visible at the object containers of the subjects that you specify during the view configuration.

- 7 Click **Data** and in the filter text box enter **Total Number of VMs**.

- 8 Select **Summary > Total Number of VMs** and double-click to add the metric.

- 9 Retain the default metric configurations and click **Save**.

## Run a vRealize Operations Manager View

To verify the view and capture a snapshot of information at any point, you run the view for a specific object.

### Prerequisites

Verify that you have the necessary access rights to perform this task. Your vRealize Operations Manager administrator can tell you which actions you can perform.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Environment** icon.

- 2 Navigate to a vCenter Server instance and click the **Details** tab.

All listed views are applicable for the vCenter Server instance.

- 3 From the **All Filters** drop-down menu on the left, select **Type > Distribution**.

You filter the views list to show only distribution type views.

- 4 Navigate to and click the **Virtual Machines Distribution** view.

The bottom pane shows the distribution view with information about this vCenter Server. Each slice represents a host and the numbers on the far left show the number of virtual machines.

## Export a vRealize Operations Manager View

To use a view in another vRealize Operations Manager, you export a content definition XML file.

If the exported view contains custom created metrics, such as what-if, supermetrics, or custom adapter metrics, you must recreate them in the new environment.

### Prerequisites

Verify that you have the necessary access rights to perform this task. Your vRealize Operations Manager administrator can tell you which actions you can perform.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Views**.
- 2 In the list of views, navigate to and click the **Virtual Machines Distribution** view .
- 3 Select **All Actions > Export view**.
- 4 Select a location on your local system to save the XML file and click **Save**.

## Import a vRealize Operations Manager View

To use views from other vRealize Operations Manager environments, you import a content definition XML file.

### Prerequisites

Verify that you have the necessary access rights to perform this task. Your vRealize Operations Manager administrator can tell you which actions you can perform.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Views**.
- 2 Select **All Actions > Import view**.
- 3 Browse to select the Virtual Machines Distribution content definition XML file and click **Import**.

If the imported view contains custom created metrics, such as what-if, supermetrics, or custom adapter metrics, you must recreate them in the new environment.

---

**Note** The imported view overwrites if a view with the same name exists. All report templates that use the existing view are updated with the imported view.

---

## Reports

A report is a scheduled snapshot of views and dashboards. You can create it to represent objects and metrics. It can contain table of contents, cover page, and footer.

With the vRealize Operations Manager reporting functions, you can generate a report to capture details related to current or predicted resource needs. You can download the report in a PDF or CSV file format for future and offline needs.



Create Reports

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_reports\\_in\\_vrom](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_reports_in_vrom))

## Report Templates Tab

On the **Report Templates** tab you can create, edit, delete, clone, run, schedule, export, and import templates.

The **Report Templates** icon is available when you select an object from the **Environment** tab in the left pane and click **Reports > Report Templates**.

All templates that are applicable for the selected object are listed on the **Report Templates** tab. You can order them by report name, subject, date they were modified, last run, or owner.

You can filter the templates list by adding a filter from the right side of the panel.

**Table 6-20. Predefined Filter Groups**

Filter Group	Description
Name	Filter by the template name. For example, you can list all reports that contain <i>my template</i> in their name by typing <b>my template</b> .
Subject	Filter by another object. If the report contains more than one view applicable for another type of object, you can filter by those objects.

vSphere users must be logged in until the report generation is complete. If you log out or your session expires, the report generation fails.

**Note** The maximum number of reports per template is 10. With every new generated report, vRealize Operations Manager deletes the oldest report.

## Generated Reports Tab

All reports that are generated for a selected object are listed on the **Generated Reports** tab.

The **Generated Reports** tab is available when you select an object from the **Environment** icon in the left pane and click **Reports > Generated Reports**.

You can order the reports by the date and time that they were created, the report name, the owner, or their status. If the report is generated through a schedule, the owner is the user who created the schedule.

**Note** The maximum number of reports per template is 10. With every new generated report, vRealize Operations Manager deletes the oldest report.

You can filter the reports list by adding a filter from the right side of the panel.

**Table 6-21. Predefined Filter Groups**

Filter Group	Description
Report Name	Filter by the report template name. For example, you can list all reports that contain <i>my template</i> in their name by typing <b>my template</b> .
Template	Filter by the report template. You can select a template from a list of templates applicable for this object.
Completion Date/Time	Filter by the date, time, or time range.
Status	Filter by the status of the report.
Subject	Filter by another object. If the report contains more than one view applicable for another type of object, you can filter by those objects.

You can download a report in a PDF or CSV format. You define the format that a report is generated in the report template.

## Create and Modify a Report Template

You create a report to generate a scheduled snapshot of views and dashboards. You can track current resources and predict potential risks to the environment. You can schedule automated reports at regular intervals.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Reports**.
- 2 On the **Report Templates** tab, click the **New Template** icon to create a template.
- 3 Complete the steps in the left pane to:
  - a Enter a name and description for the report template.  
[Name and Description Details](#)
  - b Add a view or a dashboard.  
[Views and Dashboards Details](#)
  - c Select an output for the report.  
[Formats Details](#)
  - d Select the layout options.  
[Layout Options Details](#)
- 4 Click **Save**.
- 5 From the Report Templates tab, click **Edit Template** to modify the report template.

## Name and Description Details

The name and description of the report template as they appear in the list of templates on the **Report Templates** tab.

### Where You Add Name and Description

To create or edit report templates, select **Content > Reports** in the left pane. On the Report Templates toolbar, click the plus sign to add a template or the pencil icon to edit the selected template. In the workspace, on the left, click **Name and Description**.

**Table 6-22. Name and Description Options in the Report Template Workspace**

Option	Description
Name	Name of the template as it appears on the <b>Report Templates</b> tab.
Description	Description of the template.

## Views and Dashboards Details

The report template contains views and dashboards. Views present collected information for an object. Dashboards give a visual overview of the performance and state of objects in your virtual infrastructure. You can combine different views and dashboards and order them to suit your needs.

### Where You Add Views and Dashboards

To create or edit report templates, select **Content > Reports** in the left pane. On the Report Templates toolbar, click the plus sign to add a template or the pencil icon to edit the selected template. In the workspace, on the left, click **Views and Dashboards**. If you create a new template, complete the required previous steps of the workspace.

### How You Add Views and Dashboards

To add a view or a dashboard to your report template, select it from the list on the left pane and drag it to the main panel. You can drag the views and dashboards in the main panel to reorder them. You can select portrait or landscape orientation for each view or dashboard from the drop-down menu next to its title.

**Table 6-23. Views and Dashboards Options in the Report Template Workspace**

Option	Description
Data type	Select <b>Views</b> or <b>Dashboards</b> to display a list of available views or dashboards that you can add to the template.
Create View	Create a view directly from the template workspace. This option is available when you select <b>Views</b> from the <b>Data type</b> drop-down menu.
Edit View	Edit a view directly from the template workspace. This option is available when you select <b>Views</b> from the <b>Data type</b> drop-down menu.

Option	Description
Create Dashboard	Create a dashboard directly from the template workspace. This option is available when you select <b>Dashboards</b> from the <b>Data type</b> drop-down menu.
Edit Dashboard	Edit a dashboard directly from the template workspace. This option is available when you select <b>Dashboards</b> from the <b>Data type</b> drop-down menu.
Search	Search for views or dashboards by name. To see the complete list of views or dashboards, delete the search box contents and press Enter.
List of views	List of the views that you can add to the template. This list is available when you select <b>Views</b> from the <b>Data type</b> drop-down menu.
List of dashboards	List of the dashboards that you can add to the template. This list is available when you select <b>Dashboards</b> from the <b>Data type</b> drop-down menu.
Preview of views and dashboards	In the main panel, you see a preview of the views and dashboards that you add.  When you create a template in the context of an object from the environment, you see a live preview of the views and dashboards.

## Formats Details

The formats are the outputs in which you can generate the report.

### Where You Add Formats

To create or edit report templates, select **Content > Reports** in the left pane. On the Report Templates toolbar, click the plus sign to add a template or the pencil to edit the selected template. In the workspace, on the left, click **Formats** to select a format for the report template. If you create a new template, complete the required previous steps of the workspace.

**Table 6-24. Formats Options in the Report Template Workspace**

Option	Description
PDF	With the PDF format you can read the reports, either on or off line. This format provides a page-by-page view of the reports, as they appear in printed form.
CSV	In the CSV format the data is in a structured table of lists.

## Layout Options Details

The report template can contain layout options such as cover page, table of contents, and footer.

## Where You Add Layout Options

To create or edit report templates, select **Content > Reports** in the left pane. On the Report Templates toolbar, click the plus sign to add a template or the pencil icon to edit the selected template. In the workspace, on the left, click **Layout Options**. If you create a new template, complete the required previous steps of the template.

**Table 6-25. Layout Options in the Report Template Workspace**

Option	Description
Cover Page	Can contain an image up to 5 MB. The default report size is 8.5 inches by 11 inches. The image is resized to fit the report front page.
Table of contents	Provides a list of the template parts, organized in the order of their appearance in the report.
Footer	Includes the date when the report is created, a note that the report is created by VMware vRealize Operations Manager, and page number.

## Add a Network Share Plug-In for vRealize Operations Manager Reports

You add a Network Share plug-in when you want to configure vRealize Operations Manager to send reports to a shared location.

### Prerequisites

Verify that you have read, write, and delete permissions to the network share location.

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Administration** icon.
- 2 Click **Outbound Settings** and click the plus sign to add a plug-in.
- 3 From the **Plug-In Type** drop-down menu, select **Network Share Plug-in**.

The dialog box expands to include your plug-in instance settings.

- 4 Enter an **Instance Name**.

This is the name that identifies this instance that you select when you later configure notification rules.

- 5 Configure the Network Share options appropriate for your environment.

Option	Description
<b>Domain</b>	Your shared network domain address.
<b>User Name</b>	The domain user account that is used to connect to the network.

Option	Description
Password	The password for the domain user account.
Network share root	<p>The path to the root folder where you want to save the reports. You can specify subfolders for each report when you configure the schedule publication.</p> <p>You must enter an IP address. For example, <code>\\IP_address\ShareRoot</code>. You can use the host name instead of the IP address if the host name is resolved to an IPv4 when accessed from the vRealize Operations Manager host.</p> <p><b>Note</b> Verify that the root destination folder exists. If the folder is missing, the Network Share plug-in logs an error after 5 unsuccessful attempts.</p>

- Click **Test** to verify the specified paths, credentials, and permissions.

The test might take up to a minute.

- Click **Save**.

The outbound service for this plug-in starts automatically.

- (Optional) To stop an outbound service, select an instance and click **Disable** on the toolbar.

This instance of the Network Share plug-in is configured and running.

#### What to do next

Create a report schedule and configure it to send reports to your shared folder.

## User Scenario: Handling Reports to Monitor Virtual Machines

As a virtual infrastructure administrator, you use vRealize Operations Manager to monitor several environments. You must present to your team a report with your corporate logo for all oversized and stressed virtual machines, and their current and trend memory use. You use predefined report templates to gather and format the information in a specific order.

You will create a report template with predefined views and dashboards. You will generate the report to test the template and create a schedule for generating the report once every two weeks.

#### Prerequisites

Verify that you have the necessary access rights to perform this task. Your vRealize Operations Manager administrator can tell you which actions you can perform.

#### Procedure

- [Create a Report Template for Monitoring Virtual Machines](#)

To monitor oversized and stressed virtual machines, and their memory use, you create a report template.

- [Generate a Report](#)

To generate a report, you use the Virtual Machines Report template for a vCenter Server system that shows information for oversized and stressed virtual machines, and their memory use.

### 3 Download a Report

To verify that the information appears as expected you download the generated report from the Virtual Machines Report template .

### 4 Schedule a Report

To generate a report on a selected date, time, and recurrence you create a schedule for the Virtual Machines Report template. You set the email options to send the generated report to your team.

## Create a Report Template for Monitoring Virtual Machines

To monitor oversized and stressed virtual machines, and their memory use, you create a report template.

You create a report template with PDF and CSV output and add views, dashboards and layout options to it.

### Prerequisites

- Understand the concept of vRealize Operations Manager views. See [Views](#).
- Know the location of your corporate logo.

### Procedure

#### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Content** icon and click **Reports**.
- 2 On the **Report Templates** tab, click the plus sign to create a template.
- 3 Enter **Virtual Machines Report**, the name for the template.
- 4 Enter a meaningful description for the template.

For example,

**A template for oversized and stressed virtual machines, and their memory use.**

- 5 Click **Views and Dashboards**. On the **Data type** drop-down menu leave **Views** selected.

The currently configured views are available in the list below the **Data type** drop-down menu. Views present collected information for an object in a certain way depending on the view type.

- 6 In the search box, enter **Virtual Machine**.

The list is now limited to views where the name contains Virtual Machine.

- 7 Double-click the views to add them to the template.

Option	Description
<b>Virtual Machine Rightsizing CPU, Memory, and Disk Space</b>	Monitors oversized VMs
<b>Virtual Machine Recommended CPU and Memory Size</b>	Monitors stressed VMs

The views appear in the main panel of the workspace with a preview of sample data.

- 8 In the search box, enter **VM**.

The list is now limited to views where the name contains VM.

- 9 Navigate to *VMs Memory Usage (%) Distribution* view, and double-click the view to add it to the template.

The view appears in the main panel of the workspace with a preview of sample data.

- 10 (Optional) In the main panel of the workspace, drag the views up and down to reorder them.

- 11 From the **Data type** drop-down menu, select **Dashboards**.

The currently configured dashboards appear in the list below the **Data type** drop-down menu.

Dashboards give a visual overview of the performance and state of objects in your virtual infrastructure.

- 12 Double-click **vSphere VMs Memory**, **vSphere VMs CPU**, and **vSphere VMs Disk and Network** dashboards to add them to the template.

The dashboards appear in the main panel of the workspace.

- 13 Click **Formats** and leave the **PDF** and **CSV** check boxes selected.

- 14 Click **Layout Options** and select the **Cover Page** and **Footer** check boxes.

The corresponding panes appear in the main panel of the workspace.

- 15 In the Cover Page panel, click **Browse** and navigate to an image on your computer.

The default report size is 8.5 inches by 11 inches. The image is resized to fit the report front page.

The image uploads to a database. It is used for the cover page every time you generate a report from this template.

- 16 Click **Save**.

Your report template is saved and listed on the **Report Templates** tab of the **Content** management tab.

### What to do next

Generate and download the report to verify the output. See [Generate a Report](#)

## Generate a Report

To generate a report, you use the Virtual Machines Report template for a vCenter Server system that shows information for oversized and stressed virtual machines, and their memory use.

### Prerequisites

Create a report template. See [Create a Report Template for Monitoring Virtual Machines](#).

### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Environment** icon.
- 2 Navigate to a vCenter Server system.

- 3 Click the **Reports** tab and click **Report Templates**.

The listed report templates are associated with the current object.

- 4 Navigate to the **Virtual Machines Report** template and click the **Run Template** icon.

The report is generated and listed on the **Generated Reports** tab.

#### What to do next

Download the generated report and verify the output. See [Download a Report](#).

## Download a Report

To verify that the information appears as expected you download the generated report from the Virtual Machines Report template .

#### Prerequisites

Generate a report from the Virtual Machines Report template. See [Generate a Report](#).

#### Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Environment** icon.
- 2 Navigate to the object for which you want to download a report.
- 3 Click the **Reports** tab and click **Generated Reports**.

The listed reports are generated for the current object.

- 4 Click the PDF () and CSV () icon to save the report in the relevant file format.

vRealize Operations Manager saves the report file to the location you selected.

#### What to do next

Schedule a report generation and set the email options, so your team will receive the report. See [Schedule a Report](#).

## Schedule a Report

To generate a report on a selected date, time, and recurrence you create a schedule for the Virtual Machines Report template. You set the email options to send the generated report to your team.

The date range for the generated report is based on the time when vRealize Operations Manager generates the report and not on the time when you schedule the report or when vRealize Operations Manager places the report in the queue.

#### Prerequisites

- Download the generated report to verify the output.
- To enable sending email reports, you must have configured Outbound Alert Settings.

## Procedure

- 1 In the left pane of vRealize Operations Manager, click the **Environment** icon.
- 2 Navigate to the object vCenter Server .
- 3 Click the **Reports** tab and click **Report Templates**.
- 4 Select the **Virtual Machines Report** template from the list.
- 5 Click the gear icon () and select **Schedule report**.
- 6 Select the time zone, date, and hour to start the report generation.

vRealize Operations Manager generates the scheduled reports in sequential order. Generating a report can take several hours. This process might delay the start time of a report when the previous report takes an extended period of time.

- 7 From the **Recurrence** drop-down menu, select **Weekly** and set the report generation for every two weeks on Monday.
- 8 Select the **Email report** check box to send an email with the generated report.
  - a In the **Email addresses** text box, enter the email addresses that must receive the report.
  - b Select an outbound rule.

An email is sent according to this schedule every time a report is generated.

- 9 Click **Ok**.

## What to do next

You can edit, clone, and delete report templates. Before you do, familiarize yourself with the consequences of these actions.

When you edit a report template and delete it, all reports generated from the original and the edited templates are deleted. When you clone a report template, the changes that you make to the clone do not affect the source template. When you delete a report template, all generated reports are also deleted.

# Configuring Administration Settings

# 7

After vRealize Operations Manager is installed and configured, you can use administration settings to manage your environment. You find most administration settings under the Administration selection of the vRealize Operations Manager interface.

This chapter includes the following topics:

- [Managing Users and Access Control in vRealize Operations Manager](#)
- [vRealize Operations Manager Passwords and Certificates](#)
- [Modifying Global Settings](#)
- [Create a vRealize Operations Manager Support Bundle](#)
- [Customizing Icons](#)

## Managing Users and Access Control in vRealize Operations Manager

To ensure security of the objects in your vRealize Operations Manager instance, as a system administrator you can manage all aspects of user access control. You create user accounts, assign each user to be a member of one or more user groups, and assign roles to each user or user group to set their privileges.

Users must have privileges to access specific features in the vRealize Operations Manager user interface. Access control is defined by assigning privileges to both users and objects. You can assign one or more roles to users, and enable them to perform a range of different actions on the same types of objects. For example, you can assign a user with the privileges to delete a virtual machine, and assign the same user with read-only privileges for another virtual machine.

### User Access Control

You can authenticate users in vRealize Operations Manager in several ways.

- Create local user accounts in vRealize Operations Manager.

- Use VMware vCenter Server® users. After the vCenter Server is registered with vRealize Operations Manager, configure the vCenter Server user options in the vRealize Operations Manager global settings to enable a vCenter Server user to log in to vRealize Operations Manager. When logged into vRealize Operations Manager, vCenter Server users access objects according to their vCenter Server-assigned permissions.
- Add an authentication source to authenticate imported users and user group information that resides on another machine.
  - Use LDAP to import users or user groups from an LDAP server. LDAP users can use their LDAP credentials to log in to vRealize Operations Manager.
  - Create a single sign-on source and import users and user groups from a single sign-on server. Single sign-on users can use their single sign-on credentials to log in to vRealize Operations Manager and vCenter Server. You can also use Active Directory through single sign-on by configuring the Active Directory through single sign-on and adding the single sign-on source to vRealize Operations Manager.

## User Preferences

To determine the display options for vRealize Operations Manager, such as colors for the display and health chart, the number of metrics and groups to display, and whether to synchronize system time with the host machine, you configure the user preferences on the top toolbar.

## Users of vRealize Operations Manager

Each user has an account to authenticate them when they log in to vRealize Operations Manager.

The accounts of local users and LDAP users are visible in the vRealize Operations Manager user interface when they are set up. The accounts of vCenter Server and single sign-on users only appear in the user interface after a user logs in for the first time. Each user can be assigned one or more roles, and can be an authenticated member of one or more user groups.

### Local Users in vRealize Operations Manager

When you create user accounts in a local vRealize Operations Manager instance, vRealize Operations Manager stores the credentials for those accounts in its global database, and authenticates the account user locally.

Each user account must have a unique identity, and can include any associated user preferences.

If you are logging in to vRealize Operations Manager as a local user, and on occasion receive an `invalid password` message, try the following workaround. In the Login page, change the Authentication Source to **All vCenter Servers**, change it back to **Local Users**, and log in again.

### vCenter Server Users in vRealize Operations Manager

vRealize Operations Manager supports vCenter Server users. To log in to vRealize Operations Manager, vCenter Server users must be valid users in vCenter Server.

## Roles and Associations

A vCenter Server user must have either the vCenter Server Admin role or one of the vRealize Operations Manager privileges, such as PowerUser which assigned at the root level in vCenter Server, to log in to vRealize Operations Manager. vRealize Operations Manager uses only the vCenter privileges, meaning the vRealize Operations Manager roles, at the root level, and applies them to all the objects to which the user has access. After logging in, vCenter Server users can view all the objects in vRealize Operations Manager that they can already view in vCenter Server.

## Logging in to vCenter Server Instances and Accessing Objects

vCenter Server users can access either a single vCenter Server instance or multiple vCenter Server instances, depending on the authentication source they select when they log in to vRealize Operations Manager.

- If users select a single vCenter Server instance as the authentication source, they have permission to access the objects in that vCenter Server instance. After the user has logged in, an account is created in vRealize Operations Manager with the specific vCenter Server instance serving as the authentication source.
- If users select **All vCenter Servers** as the authentication source, and they have identical credentials for each vCenter Server in the environment, they see all the objects in all the vCenter Server instances. Only users that have been authenticated by all the vCenter Servers in the environment can log in. After a user has logged in, an account is created in vRealize Operations Manager with all vCenter Server instances serving as the authentication source.

vRealize Operations Manager does not support linked vCenter Server instances. Instead, you must configure the vCenter Server adapter for each vCenter Server instance, and register each vCenter Server instance to vRealize Operations Manager.

Only objects from a specific vCenter Server instance appear in vRealize Operations Manager. If a vCenter Server instance has other linked vCenter Server instances, the data does not appear.

## vCenter Server Roles and Privileges

You cannot view or edit vCenter Server roles or privileges in vRealize Operations Manager. vRealize Operations Manager sends roles as privileges to vCenter Server as part of the vCenter Server Global privilege group. A vCenter Server administrator must assign vRealize Operations Manager roles to users in vCenter Server.

vRealize Operations Manager privileges in vCenter Server have the role appended to the name. For example, vRealize Operations Manager ContentAdmin Role, or vRealize Operations Manager PowerUser Role.

## Read-Only Principal

A vCenter Server user is a read-only principal in vRealize Operations Manager, which means that you cannot change the role, group, or objects associated with the role in vRealize Operations Manager. Instead, you must change them in the vCenter Server instance. The role applied to the root folder applies to all the objects in vCenter Server to which a user has privileges. vRealize Operations Manager does not apply individual roles on objects. For example, if a user has the PowerUser role to access the vCenter Server root folder, but has read-only access to a virtual machine, vRealize Operations Manager applies the PowerUser role to the user to access the virtual machine.

## Refreshing Permissions

When you change permissions for a vCenter Server user in vCenter Server, the user must log out and log back in to vRealize Operations Manager to refresh the permissions and view the updated results in vRealize Operations Manager. Alternatively, the user can wait for vRealize Operations Manager to refresh. The permissions refresh at fixed intervals, as defined in the `$ALIVE_BASE/user/conf/auth.properties` file. The default refreshing interval is half an hour. If necessary, you can change this interval for all nodes in the cluster.

## Single Sign-On and vCenter Users

When vCenter Server users log into vRealize Operations Manager by way of single sign-on, they are registered on the vRealize Operations Manager User Accounts page. If you delete the account of a vCenter Server user that has logged into vRealize Operations Manager by way of single sign-on, or remove the user from a single sign-on group, the user account entry still appears on the User Account page and you must delete it manually.

## Generating Reports

vCenter Server users cannot create or schedule reports in vRealize Operations Manager.

## Backward Compatibility for vCenter Server Users in vRealize Operations Manager

vRealize Operations Manager provides backward compatibility for users of the earlier version of vRealize Operations Manager, so that users of vCenter Server who have privileges in the earlier version in vCenter Server can log in to vRealize Operations Manager.

When you register vRealize Operations Manager in vCenter Server, certain roles become available in vCenter Server.

- The Administrator account in the previous version of vRealize Operations Manager maps to the PowerUser role.
- The Operator account in the previous version of vRealize Operations Manager maps to the ReadOnly role.

During registration, all roles in vRealize Operations Manager, except for vRealize Operations Manager Administrator, Maintenance, and Migration, become available dynamically in vCenter Server. Administrators in vCenter Server have all of the roles in vRealize Operations Manager that map during registration, but these administrator accounts only receive a specific role on the root folder in vCenter Server if it is specially assigned.

Registration of vRealize Operations Manager with vCenter Server is optional. If users choose not to register vRealize Operations Manager with vCenter Server, a vCenter Server administrator can still use their user name and password to log in to vRealize Operations Manager, but these users cannot use the vCenter Server session ID to log in. In this case, typical vCenter Server users must have one or more vRealize Operations Manager roles to log in to vRealize Operations Manager.

When multiple instances of vCenter Server are added to vRealize Operations Manager, user credentials become valid for all of the vCenter Server instances. When a user logs in to vRealize Operations Manager, if the user selects all vCenter Server options during login, vRealize Operations Manager requires that the user's credentials are valid for all of the vCenter Server instances. If a user account is only valid for a single vCenter Server instance, that user can select the vCenter Server instance from the login drop-down menu to log in to vRealize Operations Manager.

vCenter Server users who log in to vRealize Operations Manager must have one or more of the following roles in vCenter Server:

- vRealize Operations Content Admin Role
- vRealize Operations General User Role 1
- vRealize Operations General User Role 2
- vRealize Operations General User Role 3
- vRealize Operations General User Role 4
- vRealize Operations Power User Role
- vRealize Operations Power User without Remediation Actions Role
- vRealize Operations Read Only Role

For more information about vCenter Server users, groups, and roles, see the vCenter Server documentation.

## External User Sources in vRealize Operations Manager

You can obtain user accounts from external sources so that you can use them in your vRealize Operations Manager instance.

There are two types of external user identity sources:

- Lightweight Directory Access Protocol (LDAP): Use the LDAP source if you want to use the Active Directory or LDAP servers as authentication sources. The LDAP source does not support multi-domains even when there is a two-way trust between Domain A and Domain B.

- **Single Sign-On (SSO):** Use a single sign-on source to perform single sign-on with any application that supports vCenter single sign-on, including vRealize Operations Manager. For example, you can install a standalone vCenter Platform Services Controller (PSC) and use it to communicate with an Active Directory server. Use a PSC if the Active Directory has a setup that is too complex for the simple LDAP source in vRealize Operations Manager, or if the LDAP source is experiencing slow performance.

## Roles and Privileges in vRealize Operations Manager

vRealize Operations Manager provides several predefined roles to assign privileges to users. You can also create your own roles.

You must have privileges to access specific features in the vRealize Operations Manager user interface. The roles associated with your user account determine the features you can access and the actions you can perform.

Each predefined role includes a set of privileges for users to perform create, read, update, or delete actions on components such as dashboards, reports, administration, capacity, policies, problems, symptoms, alerts, user account management, and adapters.

<b>Administrator</b>	Includes privileges to all features, objects, and actions in vRealize Operations Manager.
<b>PowerUser</b>	Users have privileges to perform the actions of the Administrator role except for privileges to user management and cluster management. vRealize Operations Manager maps vCenter Server users to this role.
<b>PowerUserMinusRemediation</b>	Users have privileges to perform the actions of the Administrator role except for privileges to user management, cluster management, and remediation actions.
<b>ContentAdmin</b>	Users can manage all content, including views, reports, dashboards, and custom groups in vRealize Operations Manager.
<b>AgentManager</b>	Users can deploy and configure Endpoint Operations Management agents.
<b>GeneralUser-1 through GeneralUser-4</b>	These predefined template roles are initially defined as ReadOnly roles. vCenter Server administrators can configure these roles to create combinations of roles to give users multiple types of privileges. Roles are synchronized to vCenter Server once during registration.
<b>ReadOnly</b>	Users have read-only access and can perform read operations, but cannot perform write actions such as create, update, or delete.

## User Scenario: Manage User Access Control

As a system administrator or virtual infrastructure administrator, you manage user access control in vRealize Operations Manager so that you can ensure the security of your objects. Your company just

hired a new person, and you must create a user account and assign a role to the account so that the new user has permission to access specific content and objects in vRealize Operations Manager.

In this scenario you will learn how to create user accounts and roles, and assign roles to the user accounts to specify access privileges to views and objects. You will then demonstrate the intended behavior of the permissions on these accounts.

You will create a new user account, named Tom User, and a new role that grants administrative access to objects in the vRealize Operations Clusters. You will apply the new role to the user account.

Finally, you will import a user account from an external LDAP user database that resides on another machine to vRealize Operations Manager, and assign a role to the imported user account to configure the user's privileges.

### Prerequisites

Verify that the following conditions are met:

- vRealize Operations Manager is installed and operating properly, and contains objects such as clusters, hosts, and virtual machines.
- One or more user groups are defined.

### What to do next

Create a new role.

## Create a New Role

You use roles to manage access control for user accounts in vRealize Operations Manager.

In this procedure, you will add a new role and assign administrative permissions to the role.

### Prerequisites

Verify that you understand the context of this scenario. See [User Scenario: Manage User Access Control](#).

### Procedure

- 1 In vRealize Operations Manager, select **Administration** in the left pane and click **Access Control**.
- 2 Click the **Roles** tab.
- 3 Click the **Add** icon on the toolbar to create a new role.  
The **Create Role** dialog box appears.
- 4 For the role name, type **admin\_cluster**, then type a description and click **OK**.  
The **admin\_cluster** role appears in the list of roles.
- 5 Click the **admin\_cluster** role.
- 6 In the Details grid below, on the Permissions pane, click the **Edit** icon.  
The **Assign Permissions to Role** dialog box appears.

- 7 Select the **Administrative Access - all permissions** check box.
- 8 Click **Update**.

This action gives this role administrative access to all the features in the environment.

### What to do next

Create a user account, and assign this role to the account.

## Create a User Account

As an administrator you assign a unique user account to each user so that they can use vRealize Operations Manager. While you set up the user account, you assign the privileges that determine what activities the user can perform in the environment, and upon what objects.

In this procedure, you will create a user account, assign the `admin_cluster` role to the account, and associate the objects that the user can access while assigned this role. You will assign access to objects in the vRealize Operations Cluster. Then, you will test the user account to confirm that the user can access only the specified objects.

### Prerequisites

Create a new role. See [Create a New Role](#).

### Procedure

- 1 In vRealize Operations Manager, select **Administration** in the left pane and click **Access Control**.
- 2 Click the **User Accounts** tab.
- 3 Click the **Add** icon to create a new user account, and provide the information for this account.

Option	Description
<b>User Name</b>	Type the user name to use to log in to vRealize Operations Manager.
<b>Password</b>	Type a password for the user.
<b>Confirm Password</b>	Type the password again to confirm it.
<b>First Name</b>	Type the user's first name. For this scenario, type <b>Tom</b> .
<b>Last Name</b>	Type the user's last name. For this scenario, type <b>User</b> .
<b>Email Address</b>	(Optional). Type the user's email address.
<b>Description</b>	(Optional). Type a description for this user.
<b>Disable this user</b>	Do not select this check box, because you want the user to be active for this scenario.
<b>Require password change at next login</b>	Do not select this check box, because you do not need to change the user's password for this scenario.

- 4 Click **Next**.

The list of user groups appears.

- 5 Select a user group to add the user account as a member of the group.
- 6 Click the **Objects** tab.
- 7 Select the **admin\_cluster** role from the drop-down menu.
- 8 Select the **Assign this role to the user** check box.
- 9 In the Object Hierarchies list, select the **vRealize Operations Cluster** check box.
- 10 Click **Finish**.

You created a new user account for a user who can access all the vRealize Operations Cluster objects. The new user now appears in the list of user accounts.

- 11 Log out of vRealize Operations Manager.
- 12 Log in to vRealize Operations Manager as Tom User, and verify that this user account can access all the objects in the vRealize Operations Cluster hierarchy, but not other objects in the environment.
- 13 Log out of vRealize Operations Manager.

You used a specific role to assign permission to access all objects in the vRealize Operations Cluster to a user account named Tom User.

#### What to do next

Import a user account from an external LDAP user database that resides on another machine, and assign permissions to the user account.

## Import a User Account and Assign Permissions

You can import user accounts from external sources, such as an LDAP database on another machine, or a single sign-on server, so that you can give permission to those users to access certain features and objects in vRealize Operations Manager.

#### Prerequisites

- Configure an authorization source. See the vRealize Operations Manager Information Center.

#### Procedure

- 1 Log out of vRealize Operations Manager, then log in as a system administrator.
- 2 In vRealize Operations Manager, select **Administration**, and click **Access Control**.
- 3 On the toolbar, click the **Import Users** icon.
- 4 Specify the options to import user accounts from an authorization source.
  - a On the Import Users page, from the **Import From** drop-down menu, select an authentication source.
  - b In the **Domain Name** drop-down menu, type the domain name from which you want to import users, and click **Search**.
  - c Select the users you want to import, and click **Next**.

- d On the **Groups** tab, select the user group to which you want to add this user account.
  - e Click the **Objects** tab, select the **admin\_cluster** role, and select the **Assign this role to the user** check box.
  - f In the Object Hierarchies list, select the **vRealize Operations Cluster** check box, and click **Finish**.
- 5 Log out of vRealize Operations Manager.
  - 6 Log in to vRealize Operations Manager as the imported user.
  - 7 Verify that the imported user can access only the objects in the vRealize Operations Cluster.

You imported a user account from an external user database or server to vRealize Operations Manager, and assigned a role and the objects the user can access while holding this role to the user.

You have finished this scenario.

## Configure a Single Sign-On Source in vRealize Operations Manager

As a system administrator or virtual infrastructure administrator, you use single sign-on to enable SSO users to log in securely to your vRealize Operations Manager environment.

After the single sign-on source is configured, users are redirected to an SSO identity source for authentication. When logged in, users can access other vSphere components such as the vCenter Server without having to log in again.



Create Single Sign-On Source and Import User Groups in vRealize Operations Manager  
([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_create\\_sso](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_create_sso))

### Prerequisites

- Verify that the server system time of the single sign-on source and vRealize Operations Manager are synchronized. If you need to configure the Network Time Protocol (NTP), see information about cluster and node maintenance in the *vRealize Operations Manager vApp Deployment and Configuration Guide* or *vRealize Operations Manager Installation and Configuration Guide for Linux*.
- Verify that you have access to a Platform Services Controller through the vCenter Server. See the VMware vSphere Information Center for more details.

### Procedure

- 1 Log in to vRealize Operations Manager as an administrator.
- 2 Select **Administration > Authentication Sources**, and click the **Add** icon on the toolbar.

- 3 In the Add Source for User and Group Import dialog box, provide information for the single sign-on source.

Option	Action
Source Display Name	Type a name for the import source.
Source Type	Verify that SSO SAML is displayed.
Host	Enter the IP address or FQDN of the host machine where the single sign-on server resides. If you enter the FQDN of the host machine, verify that every non-remote collector node in the vRealize Operations Manager cluster can resolve the single sign-on host FQDN.
Port	Set the port to the single sign-on server listening port. By default, the port is set to 443.
User Name	Enter the user name that can log into the SSO server.
Password	Enter the password.
Grant administrator role to vRealize Operations Manager for future configuration?	Select <b>Yes</b> so that the SSO source is reregistered automatically if you make changes to the vRealize Operations Manager setup. If you select <b>No</b> , and the vRealize Operations Manager setup is changed, single sign-on users will not be able to log in until you manually reregister the single sign-on source.
Automatically redirect to vRealize Operations single sign-on URL?	Select <b>Yes</b> to direct users to the vCenter single-sign on log in page. If you select <b>No</b> , users are not redirected to SSO for authentication. This option can be changed in the vRealize Operations Manager Global Settings.
Import single sign-on user groups after adding the current source?	Select <b>Yes</b> so that the wizard directs you to the Import User Groups page when you have completed the SSO source setup. If you want to import user accounts, or user groups at a later stage, select <b>No</b> .
Advanced options	If your environment uses a load balancer, enter the IP address of the load balancer.

- 4 Click **Test** to test the source connection, and then click **OK**.

The certificate details are displayed.

- 5 Select the **Accept this Certificate** check box, and click **OK**.

- 6 In the Import User Groups dialog box, import user accounts from an SSO server on another machine.

Option	Action
Import From	Select the single sign-on server you specified when you configured the single sign-on source.
Domain Name	Select the domain name from which you want to import user groups. If Active Directory is configured as the LDAP source in the PSC, you can only import universal groups and domain local groups if the vCenter Server resides in the same domain.
Result Limit	Enter the number of results that are displayed when the search is conducted.
Search Prefix	Enter a prefix to use when searching for user groups.

- 7 In the list of user groups displayed, select at least one user group, and click **Next**.

- 8 In the Roles and Objects pane, select a role from the **Select Role** drop-down menu, and select the **Assign this role to the group** check box.
- 9 Select the objects users of the group can access when holding this role.  
To assign permissions so that users can access all the objects in vRealize Operations Manager, select the **Allow access to all objects in the system** check box.
- 10 Click **OK**.
- 11 Familiarize yourself with single-sign on and confirm that you have configured the single sign-on source correctly.
  - a Log out of vRealize Operations Manager.
  - b Log in to the vSphere Web Client as one of the users in the user group you imported from the single sign-on server.
  - c In a new browser tab, enter the IP address of your vRealize Operations Manager environment.
  - d If the single sign-on server is configured correctly, you are logged in to vRealize Operations Manager without having to enter your user credentials.

## Edit a Single Sign-On Source

Edit a single sign-on source if you need to change the administrator credentials used to manage the single sign-on source, or if you have changed the host of the source.

When you configure an SSO source, you specify either the IP address or the FQDN of the host machine where the single sign-on server resides. If you want to configure a new host, that is, if the single sign-on server resides on a different host machine than the one configured when the source was set up, vRealize Operations Manager removes the current SSO source, and creates a new source. In this case, you must reimport the users you want to associate with the new SSO source.

If you want to change the way the current host is identified in vRealize Operations Manager, for example, change the IP address to the FQDN and the reverse, or update the IP address of the PSC if the IP address of the configured PSC has changed, vRealize Operations Manager updates the current SSO source, and you are not required to reimport users.

### Procedure

- 1 Log in to vRealize Operations Manager as an administrator.
- 2 Select **Administration**, and then select **Authentication Sources**.
- 3 Select the single sign-on source and click the **Edit** icon.
- 4 Make changes to the single sign-on source, and click **OK**.  
If you are configuring a new host, the New Single Sign-On Source Detected dialog box appears.
- 5 Enter the administrator credentials that were used to set up the single sign-on source, and click **OK**.  
The current SSO source is removed, and a new one created.
- 6 Click **OK** to accept the certificate.

7 Import the users you want to associate with the SSO source.

## Audit Users and the Environment in vRealize Operations Manager

At times you might need to provide documentation as evidence of the sequence of activities that took place in your vRealize Operations Manager environment. Auditing allows you to view the users, objects, and information that is collected. To meet audit requirements, such as for business critical applications that contain sensitive data that must be protected, you can generate reports on the activities of your users, the privileges assigned to users to access objects, and the counts of objects and applications in your environment.

Auditing reports provide traceability of the objects and users in your environment.

<b>User Activity Audit</b>	Run this report to understand the scope of user activities, such as logging in, actions on clusters and nodes, changes to system passwords, activating certificates, and logging out.
<b>User Permissions Audit</b>	Generate this report to understand the scope of user accounts and their roles, access groups, and access privileges.
<b>System Audit</b>	Run this report to understand the scale of your environment. This report displays the counts of configured and collecting objects, the types and counts of adapters, configured and collecting metrics, super metrics, applications, and existing virtual environment objects. This report can help you determine whether the number of objects in your environment exceeds a supported limit.
<b>System Component Audit</b>	Run this report to display a version list of all the components in your environment.

### Reasons for Auditing Your Environment

Auditing in vRealize Operations Manager helps data center administrators in the following types of situations.

- You must track each configuration change to an authenticated user who initiated the change or scheduled the job that performed the change. For example, after an adapter changes an object, which is associated with a specific object identifier at a specific time, the data center administrator can determine the principal identifier of the authenticated user who initiated the change.
- You must track who made changes to your data center during a specific range of time, to determine who changed what on a particular day. You can identify the principal identifiers of authenticated users who were logged in to vRealize Operations Manager and running jobs, and determine who initiated the change.
- You must determine which objects were affected by a particular user during a time specific range of time.

- You must correlate events that occurred in your data center, and view these events overlaid so that you can visualize relationships and the cause of the events. Events can include login attempts, system startup and shutdown, application failures, watchdog restarts, configuration changes of applications, changes to security policy, requests, responses, and status of success.
- You must validate that the components installed in your environment are running the latest version.

## System Component Audit

A system component audit report provides a version list of every component installed in the system.

### Where You Audit System Components

To audit system components, select **Administration**, click **Audit**, and click the **System Component Audit** tab. A list of components installed in the environment appears on the page.

**Table 7-1. System Component Audit Actions**

Option	Description
Download	Display the version information in a new browser window.

## vRealize Operations Manager Passwords and Certificates

For secure vRealize Operations Manager operation, you might need to perform maintenance on passwords or authentication certificates.

- Passwords are for user access to the product interfaces or to console sessions on cluster nodes.
- Authentication certificates are for secure machine-to-machine communication within vRealize Operations Manager itself or between vRealize Operations Manager and other systems.

## Change the vRealize Operations Manager Administrator Password

You might need to change the vRealize Operations Manager administrator password as part of securing or maintaining your deployment.

### Procedure

- 1 In a Web browser, navigate to the vRealize Operations Manager administration interface at `https://master-node-name-or-ip-address/admin`.
- 2 Log in with the admin username and password for the master node.
- 3 In the upper right, click the **admin** drop-down menu, and click **Change Administrator Password**.
- 4 Enter the current password, and enter the new password twice to ensure its accuracy.

---

**Note** You cannot change the administrator username of admin.

---

- 5 Click **OK**.

## Generate a vRealize Operations Manager Passphrase

When users need to add a node to the vRealize Operations Manager cluster, you can generate a temporary passphrase instead of giving them the master administrator login credentials, which might be a security issue.

A temporary passphrase is good for one use only.

### Prerequisites

Create and configure the master node.

### Procedure

- 1 In a Web browser, navigate to the vRealize Operations Manager administration interface at `https://master-node-name-or-ip-address/admin`.
- 2 Log in with the admin username and password for the master node.
- 3 In the list of cluster nodes, select the master node.
- 4 From the toolbar above the list, click the option to generate a passphrase.
- 5 Enter a number of hours before the passphrase expires.
- 6 Click **Generate**.

A random alphanumeric string appears, which you can send to a user who needs to add a node.

### What to do next

Have the user supply the passphrase when adding a node.

## Custom vRealize Operations Manager Certificates

By default, vRealize Operations Manager includes its own authentication certificates. The default certificates cause the browser to display a warning when you connect to the vRealize Operations Manager user interface.

Your site security policies might require that you use another certificate, or you might want to avoid the warnings caused by the default certificates. In either case, vRealize Operations Manager supports the use of your own custom certificate. You can upload your custom certificate during initial master node configuration or later.

### Custom vRealize Operations Manager Certificate Requirements

A certificate used with vRealize Operations Manager must conform to certain requirements. Using a custom certificate is optional and does not affect vRealize Operations Manager features.

#### Requirements for Custom Certificates

Custom vRealize Operations Manager certificates must meet the following requirements.

- The certificate file must include the terminal (leaf) server certificate, a private key, and all issuing certificates if the certificate is signed by a chain of other certificates.

- In the file, the leaf certificate must be first in the order of certificates. After the leaf certificate, the order does not matter.
- In the file, all certificates and the private key must be in PEM format. vRealize Operations Manager does not support certificates in PFX, PKCS12, PKCS7, or other formats.
- In the file, all certificates and the private key must be PEM-encoded. vRealize Operations Manager does not support DER-encoded certificates or private keys.

PEM-encoding is base-64 ASCII and contains legible BEGIN and END markers, while DER is a binary format. Also, file extension might not match encoding. For example, a generic .cer extension might be used with PEM or DER. To verify encoding format, examine a certificate file using a text editor.

- The file extension must be .pem.
- The private key must be generated by the RSA or DSA algorithm.
- The private key must not be encrypted by a pass phrase if you use the master node configuration wizard or the administration interface to upload the certificate.
- The REST API in this vRealize Operations Manager release supports private keys that are encrypted by a pass phrase. Contact VMware Technical Support for details.
- The vRealize Operations Manager Web server on all nodes will have the same certificate file, so it must be valid for all nodes. One way to make the certificate valid for multiple addresses is with multiple Subject Alternative Name (SAN) entries.
- SHA1 certificates creates browser compatibility issues. Therefore, ensure that all certificates that are created and being uploaded to vRealize Operations Manager are signed using SHA2 or newer.
- The vRealize Operations Manager supports custom security certificates with key length up to 8192 bits. An error is displayed when you try to upload a security certificate generated with a stronger key length beyond 8192 bits.

## Verifying a Custom vRealize Operations Manager Certificate

When you upload a custom certificate file, the vRealize Operations Manager interface displays summary information for all certificates in the file.

For a valid custom certificate file, you should be able to match issuer to subject, issuer to subject, back to a self-signed certificate where the issuer and subject are the same.

In the following example, OU=MBU,O=VMware\, Inc.,CN=vc-ops-slice-32 is issued by OU=MBU,O=VMware\, Inc.,CN=vc-ops-intermediate-32, which is issued by OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca\_33717ac0-ad81-4a15-ac4e-e1806f0d3f84, which is issued by itself.

```
Thumbprint: 80:C4:84:B9:11:5B:9F:70:9F:54:99:9E:71:46:69:D3:67:31:2B:9C
Issuer Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-intermediate-32
Subject Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-slice-32
Subject Alternate Name:
PublicKey Algorithm: RSA
Valid From: 2015-05-07T16:25:24.000Z
Valid To: 2020-05-06T16:25:24.000Z
```

```

Thumbprint: 72:FE:95:F2:90:7C:86:24:D9:4E:12:EC:FB:10:38:7A:DA:EC:00:3A
Issuer Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca_33717ac0-ad81-4a15-ac4e-
e1806f0d3f84
Subject Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-intermediate-32
Subject Alternate Name: localhost,127.0.0.1
PublicKey Algorithm: RSA
Valid From: 2015-05-07T16:25:19.000Z
Valid To: 2020-05-06T16:25:19.000Z

```

```

Thumbprint: FA:AD:FD:91:AD:E4:F1:00:EC:4A:D4:73:81:DB:B2:D1:20:35:DB:F2
Issuer Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca_33717ac0-ad81-4a15-ac4e-
e1806f0d3f84
Subject Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca_33717ac0-ad81-4a15-ac4e-
e1806f0d3f84
Subject Alternate Name: localhost,127.0.0.1
PublicKey Algorithm: RSA
Valid From: 2015-05-07T16:24:45.000Z
Valid To: 2020-05-06T16:24:45.000Z

```

## Sample Contents of Custom vRealize Operations Manager Certificates

For troubleshooting purposes, you can open a custom certificate file in a text editor and inspect its contents.

### PEM Format Certificate Files

A typical PEM format certificate file resembles the following sample.

```

-----BEGIN CERTIFICATE-----
MIIF1DCCBLYgAwIBAgIKFYXYUwAAAAAAGTANBgkqhkiG9w0BAQ0FADBhMRMwEQYK
CZIMIzPyLQGBGRYDY29tMRUwEwYK CZIMIzPyLQGBGRYFdm13Y3MxGDAWBoJkiaJ
<snip>
vKStQJNr7z2+pTy92M6FgJz3y+daL+9ddbAMNp9fVXjHBoDLGGaL0vyD+KJ8+xba
aGJfGf9ELXM=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQE415ffX694riI1RmdRLJwL6s0Wa+WF70HRoLtx21kZzbXbUQN
mQhTRidJ3Ro2gRbj/btSsI+0MUzotz5VRT/yeyoTC5l2uJEapld45RroUDHQwWJ
<snip>
DAN9hQus3832xMkAuVP/jt76dHDYyviyIYbmzxMa1X7LZy1MCQVg4hCH0vLsHtLh
M1r0Asz62Eht/ib61AsVCCiN3gLrX7MKsYdxZcRVruGXSIh33ynA
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDnTCCAowGawIBAgIQY+j29InmdYNCs2cK1H4kPzANBgkqhkiG9w0BAQ0FADBh
MRMwEQYK CZIMIzPyLQGBGRYDY29tMRUwEwYK CZIMIzPyLQGBGRYFdm13Y3MxGDAW
<snip>
ukzUuqX7wEhc+QgJWgl41mWZBZ09gfsA9XuXBL0k17IpVHpEgwwrjQz8X68m4I99
dD5PF1f/nLRJvR9jwXl62yk=
-----END CERTIFICATE-----

```

### Private Keys

Private keys can appear in different formats but are enclosed with clear BEGIN and END markers.

Valid PEM sections begin with one of the following markers.

```
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN PRIVATE KEY-----
```

Encrypted private keys begin with the following marker.

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

## Bag Attributes

Microsoft certificate tools sometimes add Bag Attributes sections to certificate files. vRealize Operations Manager safely ignores content outside of BEGIN and END markers, including Bag Attributes sections.

```
Bag Attributes
Microsoft Local Key set: <No Values>
localKeyID: 01 00 00 00
Microsoft CSP Name: Microsoft RSA SChannel Cryptographic Provider
friendlyName: le-WebServer-8dea65d4-c331-40f4-aa0b-205c3c323f62
Key Attributes
X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAKHqyfc+qcQK4yxJ
om3PuB8dYZm34Qlt81GAAnBPYe3B4Q/0ba6PV8GtWG2svIpcI/eflwGHgTU3zJxR
gkKh7I3K5tGESn81ipyKtKbPbYebh+aBMqPKrNNUEKlr0M9sa3WSc0o3350tCc1ew
5ZkNYZ4BRUVYwM0HogeGh0thRn2fAgMBAECgYABhPmGN3FSZKPDG6HJlARvTLBH
KAGVnBGHd0M0mMAbghFBnBKXa8LwD1dgGBng1o0akEXTftkIjdB+uwkU5P4aRr07
vGujUtRyRCU/4fjLBDuxQL/KpQfruAQaof9uWUwh5W9fEeW3g26fzVL8AFZnbXS0
7Z0AL1H3LNclD5rPqQBANnI7vFu06bFxFV+kq6Z0JFMx7x3K4VGxgg+PffEBEPS
UJ2LuDH5/Rc63BaxFzM/q3B3Jhehvgw61mMyxU7QSSUCQC+VDuW3XEWJjSiU6KD
gEGpCyJ5SBePbLSukljPgidKkDNlKlgbWVytCVkTAmuoAz33kMwfqiNcQbUgVV
UnpzAkB7d0CP00deSsy8kMdTmKXlKf4qSF0x55epYK/5MZhBYuA1ENrR6mmjW8ke
TDNc6IGm9sVvrFBz2n9kKYpWThrJAKeAK5R69DtW0cbkLy5MqEzOHQauP36gDi1L
WMXPvUfzSYTQ5aM2rrY2/1FtSSkqUwfyh9sw8eDbqVpIV4rc6dDfcwJBALiDPT0
tz86wySJNe0iUkQm36iXVF8AckPKT9TrbC3Ho7nC80zL7gE1lEta4Zc86Z3wpcGF
BHhEDMHaihyuVgI=
-----END PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
1.3.6.1.4.1.311.17.3.92: 00 04 00 00
1.3.6.1.4.1.311.17.3.20: 7F 95 38 07 CB 0C 99 DD 41 23 26 15 8B E8
D8 4B 0A C8 7D 93
friendlyName: cos-oc-vcops
1.3.6.1.4.1.311.17.3.71: 43 00 4F 00 53 00 2D 00 4F 00 43 00 2D 00
56 00 43 00 4D 00 35 00 37 00 31 00 2E 00 76 00 6D 00 77 00 61 00
72 00 65 00 2E 00 63 00 6F 00 6D 00 00 00
1.3.6.1.4.1.311.17.3.87: 00 00 00 00 00 00 00 00 02 00 00 00 20 00
00 00 02 00 00 00 6C 00 64 00 61 00 70 00 3A 00 00 00 7B 00 41 00
45 00 35 00 44 00 44 00 33 00 44 00 30 00 2D 00 36 00 45 00 37 00
30 00 2D 00 34 00 42 00 44 00 42 00 2D 00 39 00 43 00 34 00 31 00
2D 00 31 00 43 00 34 00 41 00 38 00 44 00 43 00 42 00 30 00 38 00
42 00 46 00 7D 00 00 00 70 00 61 00 2D 00 61 00 64 00 63 00 33 00
2E 00 76 00 6D 00 77 00 61 00 72 00 65 00 2E 00 63 00 6F 00 6D 00
5C 00 56 00 4D 00 77 00 61 00 72 00 65 00 20 00 43 00 41 00 00 00
```

```

31 00 32 00 33 00 33 00 30 00 00 00
subject=/CN=cos-oc-vcops.eng.vmware.com
issuer=/DC=com/DC=vmware/CN=VMware CA
-----BEGIN CERTIFICATE-----
MIIFWTCCBEGgAwIBAgIKSJGT5gACAAAwKjANBgkqhkiG9w00BAQUFADBBMRMwEQYK
CZImiZPyLQGBGRYDY29tMRYwFAYK CZImiZPyLQGBGRYGdm13YXJlMRIwEAYDVQQD
EwIWTXdhcmUgQ0EwHhcNMTQwMjA1MTg10TM2WhcNMTYwMjA1MTg10TM2WjAmMSQw

```

## Modifying Global Settings

The global settings control the system settings for vRealize Operations Manager, including data retention and system timeout settings. You can modify one or more of the settings to monitor your environment better. These settings affect all your users.

The global settings do not affect metric interactions, color indicators, or other object management behaviors. These behaviors are configured in your policies.

Settings related to managing objects with vRealize Operations Manager are available on the **Administration > Inventory Explorer** page.

You can view tooltips for each option in the Edit Global Settings dialog box.

## Global Settings Best Practices

Most of the settings pertain to how long vRealize Operations Manager retains collected and process data.

The default values are common retention periods. You might need to adjust the time periods based on your local policies or disk space.

## List of Global Settings

The global settings determine how vRealize Operations Manager retains data, keeps connection sessions open, and other settings. These are system settings that affect all users.

**Table 7-2. Global Setting Default Values and Descriptions**

Setting	Default Value	Description
Action History	30 days	Number of days to retain the recent task data for actions. The data is purged from the system after the specified number of days.
Deleted Objects	168 hours	Number of hours to retain objects that are deleted from an adapter data source or server before deleting them from vRealize Operations Manager.  An object deleted from an adapter data source might be identified by vRealize Operations Manager as not existing and vRealize Operations Manager can no longer collect data about the object. Whether vRealize Operations Manager identifies deleted objects as not existing depends the adapter. This feature is not implemented in some adapters.  For example, if the retention time is 360 hour and a virtual machine is deleted from a vCenter Server instance, the virtual machine remains as an object in vRealize Operations Manager for 15 days before it is deleted.  This setting applies to objects deleted from the data source or server, not to any objects you delete from vRealize Operations Manager on the Inventory Explorer page.  A value of <b>-1</b> deletes objects immediately.
Deletion Schedule Interval	24 hours	Determines the frequency to schedule deletion of resources. This setting works with the Deleted Objects setting to remove objects that no longer exist in the environment. vRealize Operations Manager transparently marks objects for removal that have not existed for the length of time specified under Deleted Objects. vRealize Operations Manager then removes the marked objects at the frequency specified under Deletion Scheduling Interval.
Object History	300 days	Number of days to retain the history of the object configuration, relationship, and property data.  The configuration data is the collected data from the monitored objects on which the metrics are based. The collected data includes changes to the configuration of the object.  The data is purged from the system after the specified number of days.
Session Timeout	30 minutes	If your connection to vRealize Operations Manager is idle for the specified amount of time, you are logged out of the application. You must provide credentials to log back in.
Symptoms/Alerts	45 days	Number of days to retain canceled alerts and symptoms. The alerts and symptoms can be canceled by the system or canceled by a user.
Time Series Data	6 months	Number of months that you want to retain the collected and calculated metric data for the monitored objects.  If available disk space is less than 10%, vRealize Operations Manager purges older data and might not retain the full range specified.

Setting	Default Value	Description
Dynamic Threshold Calculation	enabled	<p>Determines whether to calculate normal levels of threshold violation for all objects.</p> <p>If the setting is disabled, the following areas of vRealize Operations Manager will not work or are not displayed:</p> <ul style="list-style-type: none"> <li>■ Anomalies badge is not calculated</li> <li>■ Alert symptom definitions based on dynamic thresholds will not work</li> <li>■ Metric charts that display normal behavior are not present</li> </ul> <p>Disable this setting only if you have no alternative options for managing resource constraints for your vRealize Operations Manager system.</p>
Capacity Calculation	enabled	<p>Determines whether to calculate capacity metrics and badges for all objects.</p> <p>If the setting is disabled, the values for the following badges are not calculated:</p> <ul style="list-style-type: none"> <li>■ Capacity Remaining</li> <li>■ Time Remaining</li> <li>■ Stress</li> <li>■ Reclaimable Capacity</li> <li>■ Density</li> </ul>
Allow vCenter Server users to log in		<p>Determine how users of vCenter Server log in to vRealize Operations Manager.</p> <ul style="list-style-type: none"> <li>■ In the vRealize Operations Manager user interface, vCenter Server users can log in to individual vCenter Server instances. Disabled by default.</li> <li>■ vCenter Server users can log in from vCenter Server clients. Enabled by default.</li> <li>■ In the vRealize Operations Manager user interface, vCenter Server users can log in to all vCenter Server instances. Enabled by default.</li> </ul>
Customer Experience Improvement Program	enabled	<p>Determines whether to participate in the Customer Experience Improvement Program by having vRealize Operations Manager send anonymous usage data to <a href="https://vmware.com">https://vmware.com</a>.</p>
Automated Actions	enabled or disabled	<p>Determines whether to allow vRealize Operations Manager to automate actions. When an alert triggers, the alert provides recommendations for remediation. You can automate an action to remediate an alert when the recommendation is the first priority for that alert. You enable actionable alerts in your policies.</p>

## Global Settings

To manage how vRealize Operations Manager retains data, keeps connection sessions open, and other settings, you can modify the values for the global settings. These system settings affect all users.

With global settings, you set times to delete objects, set timeouts, store historical data, use dynamic threshold and capacity calculations, and determine how vCenter Server users log in. For automated actions, you can select whether to allow actions to be triggered from alert recommendations automatically.

You can also choose to participate in the customer experience improvement program.

## Where You Find Global Settings

In the left pane, click the **Administration** and click **Global Settings**.

**Table 7-3. Global Settings Options**

Option	Description
Edit Global Settings	Use the toolbar option to modify setting values.
Setting	Setting name.
Value	Current value for the setting. To change the setting value, click <b>Edit Global Settings</b> .
Description	Information about the setting. Place your mouse over the setting to display additional information about the setting.

## Create a vRealize Operations Manager Support Bundle

You create a vRealize Operations Manager support bundle to gather log and configuration files for analysis when troubleshooting a vRealize Operations Manager issue.

When you create a support bundle, vRealize Operations Manager gathers files from cluster nodes into ZIP files for convenience.

### Procedure

- 1 In the left pane, click **Administration**.
- 2 Select **Support > Support Bundles**.
- 3 From the toolbar, click the button to add a support bundle.
- 4 Select the option to create a light or full support bundle.
- 5 Select the cluster nodes that need to be evaluated for support.  
Only logs from the selected nodes are included in the support bundle.
- 6 Click **OK**, and click **OK** to confirm support bundle creation.  
Depending on the size of the logs and number of nodes, it might take time for vRealize Operations Manager to create the support bundle.

### What to do next

Use the toolbar to download the support bundle ZIP files for analysis. For security, vRealize Operations Manager prompts you for credentials when you download a support bundle.

You can review the log files for error messages or, if you need troubleshooting assistance, send the diagnostic data to VMware Technical Support. When you resolve or close the issue, use the toolbar to delete the outdated support bundle to save disk space.

## Customizing Icons

Every object or adapter in your environment has an icon representation. You can customize how the icon appears.

vRealize Operations Manager assigns a default icon to each object type and adapter type. Taken collectively, object types and adapter types are known as objects in your environment. Icons represent objects in the UI and help you to identify the type of object. For example, in the Topology Graph widget on a dashboard, labeled icons show how objects are connected to one other. You can quickly identify the type of object from the icon.

If you want to differentiate objects, you can change the icon. For example, a virtual machine icon is generic. If you want to pictorially distinguish the data that a vSphere virtual machine provides from the data that a Hypervisor virtual machine provides, you can assign a different icon to each.

### Customize an Object Type Icon

You can use the default icons that vRealize Operations Manager provides, or you can upload your own graphics file for an object type. When you change an icon, your changes take effect for all users.

#### Prerequisites

If you plan to use your own icon files, verify that each image is in PNG format and has the same height and width. For best results, use a 256x256 pixel image size.

#### Procedure

- 1 Select **Content > Icons > Object Type Icons**.
- 2 Assign the Object Type icon.
  - a Select the object type in the list with the icon to change.

By default, object types for all adapter types are listed. To limit the selection to the object types that are valid for a single adapter type, select the adapter type from the drop-down menu.
  - b Click the **Upload** icon.
  - c Browse to and select the file to use and click **Done**.
- 3 (Optional) To return to the default icon, select the object type and click the **Assign Default Icons** icon.

The original default icon appears.

## Customize an Adapter Type Icon

You can use the default icons that vRealize Operations Manager provides, or you can upload your own graphics file for an adapter type. When you change an icon, your changes take effect for all users.

### Prerequisites

If you plan to use your own icon files, verify that each image is in PNG format and has the same height and width. For best results, use a 256x256 pixel image size.

### Procedure

- 1 Select **Content > Icons > Adapter Type Icons**.
- 2 Assign the Adapter Type icon.
  - a Select the adapter type in the list with the icon to change.
  - b Click the **Upload** icon.
  - c Browse to and select the file to use and click **Done**.
- 3 (Optional) To return to the default icon, select the adapter type and click the **Assign Default Icons** icon.

The original default icon appears.

# OPS-CLI Command-Line Tool

The OPS-CLI tool is a Java application that you can use to manipulate the vRealize Operations Manager database. It replaces the VCOPS-CLI and DBCLI tools.

The product includes the executable file in the tools directory or in `<VCOPS_BASE>/tools/opscli/`.

Operating System	File Name
Linux	<code>ops-cli.sh</code>
Python	<code>ops-cli.py</code>

All OPS-CLI commands use the `-h` parameter for interactive and localized help.

When you add the `control` command to the `post_install.sh` script, it triggers the `redescribe` process after an adapter is installed or upgraded.

```
control -h | redescribe --force
```

## Supported Operations

The OPS-CLI tool supports the following database operations.

- [dashboard Command Operations](#)  
You use the `dashboard` command to import, export, share, unshare, delete, reorder, show, hide, and set the default summary for dashboards.
- [template Command Operations](#)  
You use the `template` command to import, export, share, unshare, delete, and reorder templates.
- [supermetric Command Operations](#)  
You use the `supermetric` command to import, export, configure, and delete super metrics.
- [attribute Command Operations](#)  
You use the `attribute` command to configure properties of a specific metric in one or more packages. The metric is the object attribute.
- [reskind Command Operations for Object Types](#)  
You use the `reskind` command to configure the default settings in your object type as defined by the ResourceKind model element. The command sets the default attribute or supermetric package, enables or disables dynamic thresholds, and enables or disables early warning smart alerts.

- [report Command Operations](#)

You use the report command to import, export, configure, and delete super metrics.

- [view Command Operations](#)

You use the view command to import, export, or delete view definitions.

- [file Command Operations](#)

You use the file command to import, export, list or delete database files. The command operates on metric, text widget, and topology widget files.

## dashboard Command Operations

You use the dashboard command to import, export, share, unshare, delete, reorder, show, hide, and set the default summary for dashboards.

The dashboard command uses the following syntax.

```
dashboard -h | import|defsummary|export|share|unshare|delete|reorder|show|hide [parameters]
```

**Table 8-1. dashboard Command Options**

Command Name	Description	Syntax
dashboard import	Import a dashboard from a file and assign the ownership to a user account.	<pre>dashboard import -h   user-name all group:group_name input- file [--force]                 [--share all group-name[,{group- name}]] [--retry maxRetryMinutes]                 [--set rank] [--default] [--create]</pre>
dashboard export	Export an existing dashboard to a file.	<pre>dashboard export -h   user-name dashboard-name [output-dir]</pre>
dashboard defsummary	Import a dashboard from a file and assign the ownership to a user account.	<pre>dashboard defsummary -h   input-file default                 --adapterKind adapterKind -- resourceKind resourceKind</pre>
dashboard share	Share an existing dashboard with one or multiple user groups.	<pre>dashboard share -h   user-name dashboard-name all group- name[,{group-name}]</pre>
dashboard unshare	Stop sharing a dashboard with specified groups.	<pre>dashboard unshare -h   user-name dashboard-name all group- name[,{group-name}]</pre>
dashboard delete	Permanently delete a dashboard.	<pre>dashboard delete -h   user-name all group:group_name dashboard-name</pre>
dashboard reorder	Set the order rank for a dashboard, with an option to make it the default.	<pre>dashboard reorder -h   user-name all group:group_name dashboard-name                 [--set rank] [--default]</pre>

Command Name	Description	Syntax
dashboard show	Show a dashboard.	<code>dashboard show -h   user-name all group:group_name {,dashbaordname} all</code>
dashboard hide	Hide a dashboard.	<code>dashboard hide -h   user-name all group:group_name {,dashboardname} all</code>

## template Command Operations

You use the `template` command to import, export, share, unshare, delete, and reorder templates.

The `template` command uses the following syntax.

```
template -h | import|export|share|unshare|delete|reorder [parameters]
```

**Table 8-2. template Command Operations**

Command Name	Description	Syntax
template import	Import a template from a file.	<code>template import -h   input-file [--force] [--share all group-name[{{,group-name}}] [--retry maxRetryMinutes] [--set rank] [--create]</code>
template export	Export an existing template to a template file.	<code>template export -h   template-name [output-dir]</code>
template share	Share an existing template with one or multiple user groups.	<code>template share -h   template-name all group-name[{{,group-name}}]</code>
template unshare	Stop sharing a template with specified groups.	<code>template unshare -h   template-name all group-name[{{,group-name}}]</code>

Command Name	Description	Syntax
template delete	Permanently delete a template.	<code>template delete -h   template-name</code>
template reorder	Set the order rank for a template. The order rank controls the order of templates created based on shared templates.	<code>template reorder -h   template-name [--set rank]</code>

## supermetric Command Operations

You use the `supermetric` command to import, export, configure, and delete super metrics.

The `supermetric` command uses the following syntax.

```
supermetric -h | import|export|configure|delete [parameters]
```

**Table 8-3. supermetric Command Operations**

Command Name	Description	Syntax
supermetric import	Import a super metric from a file and assign the ownership to the specified user account.	<code>supermetric import -h   input-file [--force] [--policies all policy-name[,{policy-name}]] [--check (true false)] [--retry maxRetryMinutes] [--create]</code>
supermetric export	Export an existing super metric to a template file.	<code>supermetric export -h   supermetric-name [output-dir]</code>
supermetric configure	Configure properties of a super metric in one or more super metrics packages.	<code>supermetric configure -h   supermetric-name --policies all policy-name[,{policy-name}]] --check (true false) --ht (true false) --htcriticality level-name --dtabove (true false) --dtbelow (true false) --thresholds threshold-def[,{threshold-def}]</code>
supermetric delete	Permanently delete a super metric.	<code>supermetric delete -h   supermetric-name</code>

## attribute Command Operations

You use the `attribute` command to configure properties of a specific metric in one or more packages. The metric is the object attribute.

The `attribute` command uses the following syntax.

```
attribute configure -h | adapterkind-key:resourcekind-key attribute-key
    --packages all|package-name[,{package-name}] --check (true|false)
    --ht (true|false) --htcriticality level-name
    --dtabove (true|false) --dtbelow (true|false)
    --thresholds threshold-def[,{threshold-def}]
```

## reskind Command Operations for Object Types

You use the `reskind` command to configure the default settings in your object type as defined by the `ResourceKind` model element. The command sets the default attribute or supermetric package, enables or disables dynamic thresholds, and enables or disables early warning smart alerts.

The `reskind` command uses the following syntax.

```
reskind configure -h | adapterkind-key:resourcekind-key
    --package package-name --smpackage smpackagename
    --dt (true|false) --smartalert (true|false)
```

## report Command Operations

You use the `report` command to import, export, configure, and delete super metrics.

The `report` command uses the following syntax.

```
report -h | import|export|delete [parameters]
```

**Table 8-4. report Command Options**

Command Name	Description	Syntax
report import	Import a report definition from a file.	report import -h   input-file [--force]
report export	Export one or more report definitions to a file.	report export -h   all report-name[,{report-name}] [output-dir]
report delete	Permanently delete one or more report definitions.	report delete -h   all report-name[,{report-name}]

## view Command Operations

You use the `view` command to import, export, or delete view definitions.

The view command uses the following syntax.

```
view -h | import|export|delete [parameters]
```

**Table 8-5. view Command Operations**

Command Name	Description	Syntax
view import	Import a view definition from a file.	<code>view import -h   input-file [--force]</code>
view export	Export one or more view definitions to a file.	<code>view export -h   all view-name[,{,view-name}] [output-dir]</code>
view delete	Permanently delete one or more view definitions.	<code>view delete -h   all view-name[,{,view-name}]</code>

## file Command Operations

You use the file command to import, export, list or delete database files. The command operates on metric, text widget, and topology widget files.

The file command uses the following syntax.

```
file -h | import|export|delete|list [parameters]
```

**Table 8-6. file Command Operations**

Command Name	Description	Syntax
file import	Import a metric or widget from a file.	<code>file import -h   reskndmetric textwidget  topowidget input-file [--title title] [--force]</code>
file export	Export one or more metrics or text widgets, or export the topology widget to a file.	<code>file export -h   reskndmetric textwidget  topowidget all title[,{,title}] [output-dir]</code>
file delete	Permanently delete a metric or a widget.	<code>file delete -h   reskndmetric textwidget  topowidget all title[,{,title}]</code>
file list	List all metric or a widget files.	<code>file list -h   reskndmetric textwidget  topowidget</code>