vRealize Operations Manager vApp Deployment and Configuration Guide

vRealize Operations Manager 6.3

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About vApp Deployment and Configuration

The *vRealize Operations Manager vApp Deployment and Configuration Guide* provides information about deploying the VMware® vRealize Operations Manager virtual appliance, including how to create and configure the vRealize Operations Manager cluster.

The vRealize Operations Manager installation process consists of deploying the vRealize Operations Manager virtual appliance once for each cluster node, and accessing the product to finish setting up the application.

Intended Audience

This information is intended for anyone who wants to install and configure vRealize Operations Manager by using a virtual appliance deployment. The information is written for experienced virtual machine administrators who are familiar with enterprise management applications and datacenter operations.

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.

Preparing for vRealize Operations Manager Installation

1

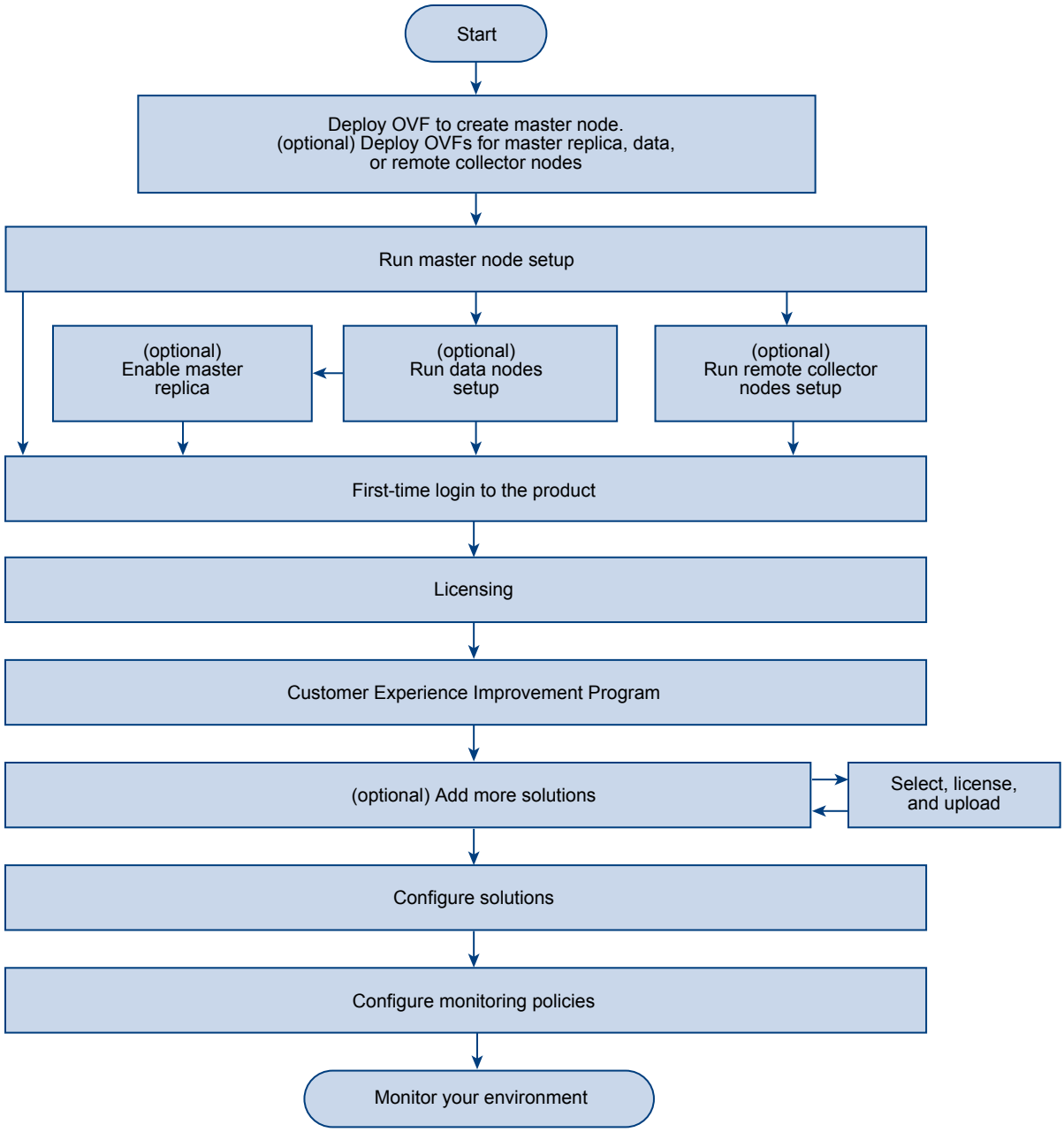
You prepare for vRealize Operations Manager installation by evaluating your environment and deploying enough vRealize Operations Manager cluster nodes to support how you want to use the product.

This chapter includes the following topics:

About vRealize Operations Manager Virtual Appliance Installation

The vRealize Operations Manager virtual appliance installation process consists of deploying the vRealize Operations Manager OVF once for each cluster node, accessing the product to set up cluster nodes according to their role, and logging in to configure the installation.

Figure 1-1. vRealize Operations Manager Installation



Complexity of Your Environment

When you deploy vRealize Operations Manager, the number and nature of the objects that you want to monitor might be complex enough to recommend a Professional Services engagement.

Complexity Levels

Every enterprise is different in terms of the systems that are present and the level of experience of deployment personnel. The following table presents a color-coded guide to help you determine where you are on the complexity scale.

- Green

  Your installation only includes conditions that most users can understand and work with, without assistance. Continue your deployment.

- Yellow

  Your installation includes conditions that might justify help with your deployment, depending on your level of experience. Consult your account representative before proceeding, and discuss using Professional Services.

- Red

  Your installation includes conditions that strongly recommend a Professional Services engagement. Consult your account representative before proceeding, and discuss using Professional Services.

Note that these color-coded levels are not firm rules. Your product experience, which increases as you work with vRealize Operations Manager and in partnership with Professional Services, must be taken into account when deploying vRealize Operations Manager.

Table 1-1. Effect of Deployment Conditions on Complexity

Complexity Level	Current or New Deployment Condition	Additional Notes
Green	You run only one vRealize Operations Manager deployment.	Lone instances are usually easy to create in vRealize Operations Manager.
Green	Your deployment includes a management pack that is listed as Green according to the compatibility guide on the VMware Solutions Exchange Web site.	The compatibility guide indicates whether the supported management pack for vRealize Operations Manager is a compatible 5.x one or a new one designed for this release. In some cases, both might work but produce different results. Regardless, users might need help in adjusting their configuration so that associated data, dashboards, alerts, and so on appear as expected. Note that the terms *solution*, *management pack*, *adapter*, and *plug-in* are used somewhat interchangeably.
Yellow	You run multiple instances of vRealize Operations Manager.	Multiple instances are typically used to address scaling or operator use patterns.

Table 1-1. Effect of Deployment Conditions on Complexity (Continued)

Complexity Level	Current or New Deployment Condition	Additional Notes
Yellow	Your deployment includes a management pack that is listed as Yellow according to the compatibility guide on the VMware Solutions Exchange Web site.	The compatibility guide indicates whether the supported management pack for vRealize Operations Manager is a compatible 5.x one or a new one designed for this release. In some cases, both might work but produce different results. Regardless, users might need help in adjusting their configuration so that associated data, dashboards, alerts, and so on appear as expected.
Yellow	You are deploying vRealize Operations Manager remote collector nodes.	Remote collector nodes gather data but leave the storage and processing of the data to the analytics cluster.
Yellow	You are deploying a multiple-node vRealize Operations Manager cluster.	Multiple nodes are typically used for scaling out the monitoring capability of vRealize Operations Manager.
Yellow	Your new vRealize Operations Manager instance will include a Linux or Windows based deployment.	Linux and Windows deployments are not as common as vApp deployments and often need special consideration.
Yellow	Your vRealize Operations Manager instance will use high availability (HA).	High availability and its node failover capability is a unique multiple-node feature that you might want additional help in understanding.
Yellow	You want help in understanding the new or changed features in vRealize Operations Manager and how to use them in your environment.	vRealize Operations Manager is different than vCenter Operations Manager in areas such as policies, alerts, compliance, custom reporting, or badges. In addition, vRealize Operations Manager uses one consolidated interface.
Red	You run multiple instances of vRealize Operations Manager, where at least one includes virtual desktop infrastructure (VDI).	Multiple instances are typically used to address scaling, operator use patterns, or because separate VDI (V4V monitoring) and non-VDI instances are needed.
Red	Your deployment includes a management pack that is listed as Red according to the compatibility guide on the VMware Solutions Exchange Web site.	The compatibility guide indicates whether the supported management pack for vRealize Operations Manager is a compatible 5.x one or a new one designed for this release. In some cases, both might work but produce different results. Regardless, users might need help in adjusting their configuration so that associated data, dashboards, alerts, and so on appear as expected.
Red	You are deploying multiple vRealize Operations Manager clusters.	Multiple clusters are typically used to isolate business operations or functions.

Table 1-1. Effect of Deployment Conditions on Complexity (Continued)

Complexity Level	Current or New Deployment Condition	Additional Notes
Red	Your current vRealize Operations Manager deployment required a Professional Services engagement to install it.	If your environment was complex enough to justify a Professional Services engagement in the previous version, it is possible that the same conditions still apply and might warrant a similar engagement for this version.
Red	Professional Services customized your vRealize Operations Manager deployment. Examples of customization include special integrations, scripting, nonstandard configurations, multiple level alerting, or custom reporting.	If your environment was complex enough to justify a Professional Services engagement in the previous version, it is possible that the same conditions still apply and might warrant a similar engagement for this version.

vRealize Operations Manager Cluster Nodes

All vRealize Operations Manager clusters consist of a master node, an optional replica node for high availability, optional data nodes, and optional remote collector nodes.

When you install vRealize Operations Manager, you use a vRealize Operations Manager vApp deployment, Linux installer, or Windows installer to create role-less nodes. After the nodes are created and have their names and IP addresses, you use an administration interface to configure them according to their role.

You can create role-less nodes all at once or as needed. A common as-needed practice might be to add nodes to scale out vRealize Operations Manager to monitor an environment as the environment grows larger.

The following node types make up the vRealize Operations Manager analytics cluster:

Master Node The initial, required node in vRealize Operations Manager. All other nodes are managed by the master node.

In a single-node installation, the master node manages itself, has adapters installed on it, and performs all data collection and analysis.

Data Node In larger deployments, additional data nodes have adapters installed and perform collection and analysis.

Larger deployments usually include adapters only on the data nodes so that master and replica node resources can be dedicated to cluster management.

Replica Node To use vRealize Operations Manager high availability (HA), the cluster requires that you convert a data node into a replica of the master node.

The following node type is a member of the vRealize Operations Manager cluster but not part of the analytics cluster:

Remote Collector Node Distributed deployments might require a remote collector node that can navigate firewalls, interface with a remote data source, reduce bandwidth across data centers, or reduce the load on the vRealize Operations Manager analytics cluster. Remote collectors only gather objects for the inventory, without storing data or performing analysis. In addition, remote collector nodes may be installed on a different operating system than the rest of the cluster.

General vRealize Operations Manager Cluster Node Requirements

When you create the cluster nodes that make up vRealize Operations Manager, you have general requirements that you must meet.

General Requirements

- vRealize Operations Manager Version. All nodes must run the same vRealize Operations Manager version.

  For example, do not add a version 6.1 data node to a cluster of vRealize Operations Manager 6.2 nodes.

- Analytics Cluster Deployment Type. In the analytics cluster, all nodes must be the same kind of deployment: vApp, Linux, or Windows.

  Do not mix vApp, Linux, and Windows nodes in the same analytics cluster.

- Remote Collector Deployment Type. A remote collector node does not need to be the same deployment type as the analytics cluster nodes.

  When you add a remote collector of a different deployment type, the following combinations are supported:

  - vApp analytics cluster and Windows remote collector
  - Linux analytics cluster and Windows remote collector

- Analytics Cluster Node Sizing. In the analytics cluster, CPU, memory, and disk size must be identical for all nodes.

  Master, replica, and data nodes must be uniform in sizing.

- Remote Collector Node Sizing. Remote collector nodes may be of different sizes from each other or from the uniform analytics cluster node size.

- Geographical Proximity. You may place analytics cluster nodes in different vSphere clusters, but the nodes must reside in the same geographical location.

  Different geographical locations are not supported.

- Virtual Machine Maintenance. When any node is a virtual machine, you may only update the virtual machine software by directly updating the vRealize Operations Manager software.

  For example, going outside of vRealize Operations Manager to access vSphere to update VMware Tools is not supported.

- Redundancy and Isolation. If you expect to enable HA, place analytics cluster nodes on separate hosts. See "About vRealize Operations Manager High Availability," on page 27.

Requirements for Solutions

Be aware that solutions might have requirements beyond those for vRealize Operations Manager itself. For example, vRealize Operations Manager for Horizon View has specific sizing guidelines for its remote collectors.

See your solution documentation, and verify any additional requirements before installing solutions. Note that the terms *solution*, *management pack*, *adapter*, and *plug-in* are used somewhat interchangeably.

vRealize Operations Manager Cluster Node Networking Requirements

When you create the cluster nodes that make up vRealize Operations Manager, the associated setup within your network environment is critical to inter-node communication and proper operation.

Networking Requirements

Important vRealize Operations Manager analytics cluster nodes need frequent communication with one another. In general, your underlying vSphere architecture might create conditions where some vSphere actions affect that communication. Examples include, but are not limited to, vMotions, storage vMotions, HA events, and DRS events.

- The master and replica nodes must be addressed by static IP address, or fully qualified domain name (FQDN) with a static IP address.

  Data and remote collector nodes may use dynamic host control protocol (DHCP).

- You must be able to successfully reverse-DNS all nodes, including remote collectors, to their FQDN, currently the node hostname.

  Nodes deployed by OVF have their hostnames set to the retrieved FQDN by default.

- All nodes, including remote collectors, must be bidirectionally routable by IP address or FQDN.
- Analytics cluster nodes must not be separated by network address translation (NAT), load balancer, firewall, or a proxy that inhibits bidirectional communication by IP address or FQDN.
- Analytics cluster nodes must not have the same hostname.
- Place analytics cluster nodes within the same data center and connect them to the same local area network (LAN).
- Place analytics cluster nodes on same Layer 2 network and IP subnet.

  A stretched Layer 2 or routed Layer 3 network is not supported.

- Do not span the Layer 2 network across sites, which might create network partitions or network performance issues.
- One-way latency between analytics cluster nodes must be 5 ms or lower.
- Network bandwidth between analytics cluster nodes must be 1 gbps or higher.
- Do not distribute analytics cluster nodes over a wide area network (WAN).

  To collect data from a WAN, a remote or separate data center, or a different geographic location, use remote collectors.

- Remote collectors are supported through a routed network but not through NAT.

vRealize Operations Manager Cluster Node Best Practices

When you create the cluster nodes that make up vRealize Operations Manager, additional best practices improve performance and reliability in vRealize Operations Manager.

Best Practices

- Deploy vRealize Operations Manager analytics cluster nodes in the same vSphere cluster.

- If you deploy analytics cluster nodes in a highly consolidated vSphere cluster, you might need resource reservations for optimal performance.

  Determine whether the virtual to physical CPU ratio is affecting performance by reviewing CPU ready time and co-stop.
- Deploy analytics cluster nodes on the same type of storage tier.
- To continue to meet analytics cluster node size and performance requirements, apply storage DRS anti-affinity rules so that nodes are on separate datastores.
- To prevent unintentional migration of nodes, set storage DRS to manual.
- To ensure balanced performance from analytics cluster nodes, use ESXi hosts with the same processor frequencies. Mixed frequencies and physical core counts might affect analytics cluster performance.
- To avoid a performance decrease, vRealize Operations Manager analytics cluster nodes need guaranteed resources when running at scale. The vRealize Operations Manager Knowledge Base includes sizing spreadsheets that calculate resources based on the number of objects and metrics that you expect to monitor, use of HA, and so on. When sizing, it is better to over-allocate than under-allocate resources.

  See Knowledge Base article 2093783.
- Because nodes might change roles, avoid machine names such as Master, Data, Replica, and so on. Examples of changed roles might include making a data node into a replica for HA, or having a replica take over the master node role.
- The NUMA placement is removed in the vRealize Operations Manager 6.3 and later. Procedures related to NUMA settings from the OVA file follow:

Table 1-2. NUMA Setting

Action	Description
Set the vRealize Operations Manager cluster status to offline	1 Shut down the vRealize Operations Manager cluster. 2 Right-click the cluster and click **Edit Settings > Options > Advanced General**. 3 Click **Configuration Parameters**. In the vSphere Client, repeat these steps for each VM.
Remove the NUMA setting	1 From the Configuration Parameters, remove the setting `numa.vcpu.preferHT` and click **OK**. 2 Click **OK**. 3 Repeat these steps for all the VMs in the vRealize Operations cluster. 4 Power on the cluster.

Note To ensure the availability of adequate resources and continued product performance, monitor vRealize Operations performance by checking its CPU usage, CPU ready and CPU contention time.

Using IPv6 with vRealize Operations Manager

vRealize Operations Manager supports Internet Protocol version 6 (IPv6), the network addressing convention that will eventually replace IPv4. Use of IPv6 with vRealize Operations Manager requires that certain limitations be observed.

Using IPv6

- All vRealize Operations Manager cluster nodes, including remote collectors, must have IPv6 addresses. Do not mix IPv6 and IPv4.

- All vRealize Operations Manager cluster nodes, including remote collectors, must be vApp or Linux based. vRealize Operations Manager for Windows does not support IPv6.
- Use global IPv6 addresses only. Link-local addresses are not supported.
- If any nodes use DHCP, your DHCP server must be configured to support IPv6.
- DHCP is only supported on data nodes and remote collectors. Master nodes and replica nodes still require fixed addresses, which is true for IPv4 as well.
- Your DNS server must be configured to support IPv6.
- When adding nodes to the cluster, remember to enter the IPv6 address of the master node.
- When registering a VMware vCenter® instance within vRealize Operations Manager, place square brackets around the IPv6 address of your VMware vCenter Server® system if vCenter is also using IPv6.

  For example: `[2015:0db8:85a3:0042:1000:8a2e:0360:7334]`

  Note that, even when vRealize Operations Manager is using IPv6, vCenter Server may still have an IPv4 address. In that case, vRealize Operations Manager does not need the square brackets.
- You cannot register an Endpoint Operations Management agent in an environment that supports both IPv4 and IPv6. In the event that you attempt to do so, the following error appears:

  ```
  Connection failed. Server may be down (or wrong IP/port were used). Waiting for 10 seconds
  before retrying.
  ```

Sizing the vRealize Operations Manager Cluster

The resources needed for vRealize Operations Manager depend on how large of an environment you expect to monitor and analyze, how many metrics you plan to collect, and how long you need to store the data.

It is difficult to broadly predict the CPU, memory, and disk requirements that will meet the needs of a particular environment. There are many variables, such as the number and type of objects collected, which includes the number and type of adapters installed, the presence of HA, the duration of data retention, and the quantity of specific data points of interest, such as symptoms, changes, and so on.

VMware expects vRealize Operations Manager sizing information to evolve, and maintains Knowledge Base articles so that sizing calculations can be adjusted to adapt to usage data and changes in versions of vRealize Operations Manager.

Knowledge Base article 2093783

The Knowledge Base articles include overall maximums, plus spreadsheet calculators in which you enter the number of objects and metrics that you expect to monitor. To obtain the numbers, some users take the following high-level approach, which uses vRealize Operations Manager itself.

1. Review this guide to understand how to deploy and configure a vRealize Operations Manager node.
2. Deploy a temporary vRealize Operations Manager node.
3. Configure one or more adapters, and allow the temporary node to collect overnight.
4. Access the Cluster Management page on the temporary node.
5. Using the Adapter Instances list in the lower portion of the display as a reference, enter object and metric totals of the different adapter types into the appropriate sizing spreadsheet from Knowledge Base article 2093783.
6. Deploy the vRealize Operations Manager cluster based on the spreadsheet sizing recommendation. You can build the cluster by adding resources and data nodes to the temporary node or by starting over.

If you have a large number of adapters, you might need to reset and repeat the process on the temporary node until you have all the totals you need. The temporary node will not have enough capacity to simultaneously run every connection from a large enterprise.

Another approach to sizing is through self monitoring. Deploy the cluster based on your best estimate, but create an alert for when capacity falls below a threshold, one that allows enough time to add nodes or disk to the cluster. You also have the option to create an email notification when thresholds are passed.

During internal testing, a single-node vApp deployment of vRealize Operations Manager that monitored 8,000 virtual machines ran out of disk storage within one week.

Add Data Disk Space to a vRealize Operations Manager vApp Node

You add to the data disk of vRealize Operations Manager vApp nodes when space for storing the collected data runs low.

Prerequisites

- Note the disk size of the analytics cluster nodes. When adding disk, you must maintain uniform size across analytics cluster nodes.
- Use the vRealize Operations Manager administration interface to take the node offline.
- Verify that you are connected to a vCenter Server system with a vSphere client, and log in to the vSphere client.

Procedure

1 Shut down the virtual machine for the node.

2 Edit the hardware settings of the virtual machine, and do one of the following:

- Increase the size of **Hard Disk 2**.

  You cannot increase the size when the virtual machine has snapshots.

- Add another disk.

3 Power on the virtual machine for the node.

During the power-on process, the virtual machine expands the vRealize Operations Manager data partition.

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.

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
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFdm13Y3MxGDAWBgoJkiaJ
<snip>
vKStQJNr7z2+pTy92M6FgJz3y+daL+9ddbaMNp9fVXjHBoDLGGaLOvyD+KJ8+xba
aGJfGf9ELXM=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4l5ffX694riI1RmdRLJwL6sOWa+Wf70HRoLtx21kZzbXbUQN
mQhTRiidJ3Ro2gRbj/btSsI+OMUzotz5VRT/yeyoTC5l2uJEapld45RroUDHQwWJ
<snip>
DAN9hQus3832xMkAuVP/jt76dHDYyviyIYbmxzMalX7LZy1MCQVg4hCH0vLsHtLh
M1rOAsz62Eht/iB61AsVCCiN3gLrX7MKsYdxZcRVruGXSIh33ynA
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDnTCCAoWgAwIBAgIQY+j29InmdYNCs2cK1H4kPzANBgkqhkiG9w0BAQ0FADBh
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFdm13Y3MxGDAW
<snip>
ukzUuqX7wEhc+QgJWgl41mWZBZ09gfsA9XuXBL0k17IpVHpEgwwrjQz8X68m4I99
dD5Pflf/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/0ba6PV8GtWG2svIpcl/eflwGHgTU3zJxR
gkKh7I3K5tGESn81ipyKTkPbYebh+aBMqPKrNNUEKlr0M9sa3WSc0o3350tCc1ew
5ZkNYZ4BRUVYWm0HogeGhOthRn2fAgMBAAECgYABhPmGN3FSZKPDG6HJlARvTlBH
KAGVnBGHd0MOmMAbghFBnBKXa8LwD1dgGBng1oOakEXTftkIjdB+uwkU5P4aRrO7
vGujUtRyRCU/4fjLBDuxQL/KpQfruAQaof9uWUwh5W9fEeW3g26fzVL8AFZnbXS0
7Z0AL1H3LNcLd5rpOQJBANnI7vFu06bFxVF+kq6ZOJFMx7x3K4VGxgg+PfFEBEPS
UJ2LuDH5/Rc63BaxFzM/q3B3Jhehvgw61mMyxU7QSSUCQQC+VDuW3XEWJjSiU6KD
gEGpCyJ5SBePbLSukljpGidKkDNlkLgbWVytCVkTAmuoAz33kMWfqIiNcqQbUgVV
UnpzAkB7d0CPO0deSsy8kMdTmKXLKf4qSF0x55epYK/5MZhBYuA1ENrR6mmjW8ke
TDNc6IGm9sVvrFBz2n9kKYpWThrJAkEAk5R69DtW0cbkLy5MqEzOHQauP36gDi1L
WMXPvUfzSYTQ5aM2rrY2/1FtSSkqUwfYh9sw8eDbqVpIV4rc6dDfcwJBALiiDPT0
tz86wySJNeOiUkQm36iXVF8AckPKT9TrbC3Ho7nC8OzL7gEllETa4Zc86Z3wpcGF
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-----
MIIFWTCCBEGgAwIBAgIKSJGT5gACAAAwKjANBgkqhkiG9w0BAQUFADBBMRMwEQYK
CZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGdm13YXJlMRIwEAYDVQQD
EwlWTXdhcmUgQ0EwHhcNMTQwMjA1MTg1OTM2WhcNMTYwMjA1MTg1OTM2WjAmMSQw
```

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
```

Create a Node by Deploying an OVF

vRealize Operations Manager consists of one or more nodes, in a cluster. To create nodes, you use the vSphere client to download and deploy the vRealize Operations Manager virtual machine, once for each cluster node.

Prerequisites

- Verify that you have permissions to deploy OVF templates to the inventory.
- If the ESXi host is part of a cluster, enable DRS in the cluster. If an ESXi host belongs to a non-DRS cluster, all resource pool functions are disabled.

- If this node is to be the master node, reserve a static IP address for the virtual machine, and know the associated domain name server, default gateway, and network mask values.

  Plan to keep the IP address because it is difficult to change the address after installation.

- If this node is to be a data node that will become the HA replica node, reserve a static IP address for the virtual machine, and know the associated domain name server, default gateway, and network mask values.

  Plan to keep the IP address because it is difficult to change the address after installation.

  In addition, familiarize yourself with HA node placement as described in "About vRealize Operations Manager High Availability," on page 27.

- Preplan your domain and machine naming so that the deployed virtual machine name will begin and end with alphabet (a–z) or digit (0–9) characters, and will only contain alphabet, digit, or hyphen (-) characters. The underscore character (_) must not appear in the host name or anywhere in the fully qualified domain name (FQDN).

  Plan to keep the name because it is difficult to change the name after installation.

  For more information, review the host name specifications from the Internet Engineering Task Force. See www.ietf.org.

- Preplan node placement and networking to meet the requirements described in "General vRealize Operations Manager Cluster Node Requirements," on page 12 and "vRealize Operations Manager Cluster Node Networking Requirements," on page 13.

- If you expect the vRealize Operations Manager cluster to use IPv6 addresses, review the IPv6 limitations described in "Using IPv6 with vRealize Operations Manager," on page 14.

- Download the vRealize Operations Manager `.ova` file to a location that is accessible to the vSphere client.

- If you download the virtual machine and the file extension is `.tar`, change the file extension to `.ova`.

- Verify that you are connected to a vCenter Server system with a vSphere client, and log in to the vSphere client.

  Do not deploy vRealize Operations Manager from an ESXi host. Deploy only from vCenter Server.

Procedure

1. Select the vSphere **Deploy OVF Template** option.
2. Enter the path to the vRealize Operations Manager `.ova` file.
3. Follow the prompts until you are asked to enter a name for the node.
4. Enter a node name. Examples might include **`Ops1`**, **`Ops2`** or **`Ops-A`**, **`Ops-B`**.

   Do not include nonstandard characters such as underscores (_) in node names.

   Use a different name for each vRealize Operations Manager node.
5. Follow the prompts until you are asked to select a configuration size.
6. Select the size configuration that you need. Your selection does not affect disk size.

   Default disk space is allocated regardless of which size you select. If you need additional space to accommodate the expected data, add more disk after deploying the vApp.

7 Follow the prompts until you are asked to select the disk format.

Option	Description
Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format.
Thick Provision Eager Zeroed	Creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Thick provisioned eager-zeroed format can improve performance depending on the underlying storage subsystem. Select the thick provisioned eager-zero option when possible.
Thin Provision	Creates a disk in thin format. Use this format to save storage space.

Snapshots can negatively affect the performance of a virtual machine and typically result in a 25–30 percent degradation for the vRealize Operations Manager workload. Do not use snapshots.

8 Click **Next**.

9 From the drop-down menu, select a Destination Network, for example, **Network 1 = TEST**, and click **Next**.

10 In Properties, under Application, Timezone Setting, leave the default of UTC or select a time zone.

The preferred approach is to standardize on UTC. Alternatively, configure all nodes to the same time zone.

11 (Optional) Select the option for IPv6.

12 Under Networking Properties, leave the entries blank for DHCP, or fill in the default gateway, domain name server, static IP address, and network mask values.

The master node and replica node require a static IP. A data node or remote collector node may use DHCP or static IP.

13 Click **Next**.

14 Review the settings and click **Finish**.

15 If you are creating a multiple-node vRealize Operations Manager cluster, repeat Step 1 through Step 14 to deploy each node.

What to do next

Use a Web browser client to configure a newly added node as the vRealize Operations Manager master node, a data node, a high availability master replica node, or a remote collector node. The master node is required first.

Caution For security, do not access vRealize Operations Manager from untrusted or unpatched clients, or from clients using browser extensions.

Creating the vRealize Operations Manager Master Node

2

All vRealize Operations Manager installations require a master node.

This chapter includes the following topics:

About the vRealize Operations Manager Master Node

The master node is the required, initial node in your vRealize Operations Manager cluster.

In single-node clusters, administration and data are on the same master node. A multiple-node cluster includes one master node and one or more data nodes. In addition, there might be remote collector nodes, and there might be one replica node used for high availability.

The master node performs administration for the cluster and must be online before you configure any new nodes. In addition, the master node must be online before other nodes are brought online. If the master node and replica node go offline together, bring them back online separately. Bring the master node completely online first, and then bring the replica node online. For example, if the entire cluster were offline for any reason, you would bring the master node online first.

Creating the Master Node (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_create_master_node)

Run the Setup Wizard to Create the Master Node

All vRealize Operations Manager installations require a master node. With a single node cluster, administration and data functions are on the same master node. A multiple-node vRealize Operations Manager cluster contains one master node and one or more nodes for handling additional data.

Prerequisites

- Create a node by deploying the vRealize Operations Manager vApp.
- After it is deployed, note the fully qualified domain name (FQDN) or IP address of the node.
- If you plan to use a custom authentication certificate, verify that your certificate file meets the requirements for vRealize Operations Manager. See "Custom vRealize Operations Manager Certificates," on page 16.

Procedure

1 Navigate to the name or IP address of the node that will be the master node of vRealize Operations Manager.

The setup wizard appears, and you do not need to log in to vRealize Operations Manager.

2 Click **New Installation**.

3 Click **Next**.

4 Enter and confirm a password for the admin user account, and click **Next**.

Passwords require a minimum of 8 characters, one uppercase letter, one lowercase letter, one digit, and one special character.

The user account name is admin by default and cannot be changed.

5 Select whether to use the certificate included with vRealize Operations Manager or to install one of your own.

a To use your own certificate, click **Browse**, locate the certificate file, and click **Open** to load the file in the Certificate Information text box.

b Review the information detected from your certificate to verify that it meets the requirements for vRealize Operations Manager.

6 Click **Next**.

7 Enter a name for the master node.

For example: **`Ops-Master`**

8 Enter the URL or IP address for the Network Time Protocol (NTP) server with which the cluster will synchronize.

For example: **`time.nist.gov`**

9 Click **Add**.

Leave the NTP blank to have vRealize Operations Manager manage its own synchronization by having all nodes synchronize with the master node and replica node.

10 Click **Next**, and click **Finish**.

The administration interface appears, and it takes a moment for vRealize Operations Manager to finish adding the master node.

What to do next

After creating the master node, you have the following options.

- Create and add data nodes to the unstarted cluster.
- Create and add remote collector nodes to the unstarted cluster.
- Click **Start vRealize Operations Manager** to start the single-node cluster, and log in to finish configuring the product.

  The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.

Scaling vRealize Operations Manager Out by Adding a Data Node 3

You can deploy and configure additional nodes so that vRealize Operations Manager can support larger environments.

This chapter includes the following topics:

About vRealize Operations Manager Data Nodes

Data nodes are the additional cluster nodes that allow you to scale out vRealize Operations Manager to monitor larger environments.

A data node always shares the load of performing vRealize Operations Manager analysis and might also have a solution adapter installed to perform collection and data storage from the environment. You must have a master node before you add data nodes.

You can dynamically scale out vRealize Operations Manager by adding data nodes without stopping the vRealize Operations Manager cluster. When you scale out the cluster by 25% or more, you should restart the cluster to allow vRealize Operations Manager to update its storage size, and you might notice a decrease in performance until you restart. A maintenance interval provides a good opportunity to restart the vRealize Operations Manager cluster.

In addition, the product administration options include an option to re-balance the cluster, which can be done without restarting. Rebalancing adjusts the vRealize Operations Manager workload across the cluster nodes.

Note Do not shut down online cluster nodes externally or by using any means other than the vRealize Operations Manager interface. Shut down a node externally only after taking it offline in the vRealize Operations Manager interface.

Creating a Data Node (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_create_data_node)

Run the Setup Wizard to Add a Data Node

Larger environments with multiple-node vRealize Operations Manager clusters contain one master node and one or more data nodes for additional data collection, storage, processing, and analysis.

Prerequisites

- Create nodes by deploying the vRealize Operations Manager vApp.

- Create and configure the master node.
- Note the fully qualified domain name (FQDN) or IP address of the master node.

Procedure

1 In a Web browser, navigate to the name or IP address of the node that will become the data node.

  The setup wizard appears, and you do not need to log in to vRealize Operations Manager.

2 Click **Expand an Existing Installation**.

3 Click **Next**.

4 Enter a name for the node (for example, **`Data-1`**).

5 From the Node Type drop-down, select **Data**.

6 Enter the FQDN or IP address of the master node and click **Validate**.

7 Select **Accept this certificate** and click **Next**.

  If necessary, locate the certificate on the master node and verify the thumbprint.

8 Verify the vRealize Operations Manager administrator username of admin.

9 Enter the vRealize Operations Manager administrator password.

  Alternatively, instead of a password, type a pass-phrase that you were given by your vRealize Operations Manager administrator.

10 Click **Next**, and click **Finish**.

  The administration interface appears, and it takes a moment for vRealize Operations Manager to finish adding the data node.

What to do next

After creating a data node, you have the following options.

- New, unstarted clusters:
  - Create and add more data nodes.
  - Create and add remote collector nodes.
  - Create a high availability master replica node.
  - Click **Start vRealize Operations Manager** to start the cluster, and log in to finish configuring the product.

    The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.
- Established, running clusters:
  - Create and add more data nodes.
  - Create and add remote collector nodes.
  - Create a high availability master replica node, which requires a cluster restart.

Adding High Availability to vRealize Operations Manager

4

You can dedicate one vRealize Operations Manager cluster node to serve as a replica node for the vRealize Operations Manager master node.

This chapter includes the following topics:

About vRealize Operations Manager High Availability

vRealize Operations Manager supports high availability (HA). HA creates a replica for the vRealize Operations Manager master node and protects the analytics cluster against the loss of a node.

With HA, data stored on the master node is always 100% backed up on the replica node. To enable HA, you must have at least one data node deployed, in addition to the master node.

- HA is not a disaster recovery mechanism. HA protects the analytics cluster against the loss of only one node, and because only one loss is supported, you cannot stretch nodes across vSphere clusters in an attempt to isolate nodes or build failure zones.
- When HA is enabled, the replica can take over all functions that the master provides, were the master to fail for any reason. If the master fails, failover to the replica is automatic and requires only two to three minutes of vRealize Operations Manager downtime to resume operations and restart data collection.

  When a master node problem causes failover, the replica node becomes the master node, and the cluster runs in degraded mode. To get out of degraded mode, take one of the following steps.

  - Return to HA mode by correcting the problem with the master node, which allows vRealize Operations Manager to configure the node as the new replica node.
  - Return to HA mode by converting a data node into a new replica node and then removing the old, failed master node. Removed master nodes cannot be repaired and re-added to vRealize Operations Manager.
  - Change to non-HA operation by disabling HA and then removing the old, failed master node. Removed master nodes cannot be repaired and re-added to vRealize Operations Manager.
- In the administration interface, after an HA replica node takes over and becomes the new master node, you cannot remove the previous, offline master node from the cluster. In addition, the previous node continues to be listed as a master node. To refresh the display and enable removal of the node, refresh the browser.

- When HA is enabled, the cluster can survive the loss of one data node without losing any data. However, HA protects against the loss of only one node at a time, of any kind, so simultaneously losing data and master/replica nodes, or two or more data nodes, is not supported. Instead, vRealize Operations Manager HA provides additional application level data protection to ensure application level availability.
- When HA is enabled, it lowers vRealize Operations Manager capacity and processing by half, because HA creates a redundant copy of data throughout the cluster, as well as the replica backup of the master node. Consider your potential use of HA when planning the number and size of your vRealize Operations Manager cluster nodes. See "Sizing the vRealize Operations Manager Cluster," on page 15.
- When HA is enabled, deploy analytics cluster nodes on separate hosts for redundancy and isolation. One option is to use anti-affinity rules that keep nodes on specific hosts in the vSphere cluster.

  If you cannot keep the nodes separate, you should not enable HA. A host fault would cause the loss of more than one node, which is not supported, and all of vRealize Operations Manager would become unavailable.

  The opposite is also true. Without HA, you could keep nodes on the same host, and it would not make a difference. Without HA, the loss of even one node would make all of vRealize Operations Manager unavailable.
- When you power off the data node and change the network settings of the VM, this affects the IP address of the data node. After this point, the HA cluster is no longer accessible and all the nodes have a status of "Waiting for analytics". Verify that you have used a static IP address.

Creating a Replica Node for High Availability (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_create_replica_node_ha)

Run the Setup Wizard to Add a Master Replica Node

You can convert a vRealize Operations Manager data node to a replica of the master node, which adds high availability (HA) for vRealize Operations Manager.

Note If the cluster is running, enabling HA restarts the cluster.

If you convert a data node that is already in use for data collection and analysis, adapters and data connections that were provided through that data node fail over to other data nodes.

You may add HA to the vRealize Operations Manager cluster at installation time or after vRealize Operations Manager is up and running. Adding HA at installation is less intrusive because the cluster has not yet started.

Prerequisites

- Create nodes by deploying the vRealize Operations Manager vApp.
- Create and configure the master node.
- Create and configure a data node with a static IP address.
- Note the fully qualified domain name (FQDN) or IP address of the master node.

Procedure

1 In a Web browser, navigate to the master node administration interface.

  `https://`*`master-node-name-or-ip-address`*`/admin`

2 Enter the vRealize Operations Manager administrator username of **`admin`**.

3 Enter the vRealize Operations Manager administrator password and click **Log In**.

4 Under High Availability, click **Enable**.

5 Select a data node to serve as the replica for the master node.

6 Select the **Enable High Availability for this cluster** option, and click **OK**.

If the cluster was online, the administration interface displays progress as vRealize Operations Manager configures, synchronizes, and rebalances the cluster for HA.

7 If the master node and replica node go offline, and the master remains offline for any reason while the replica goes online, the replica node does not take over the master role, take the entire cluster offline, including data nodes and log in to the replica node command line console as a root.

8 Open `$ALIVE_BASE/persistence/persistence.properties` in a text editor.

9 Locate and set the following properties:

```
db.role=MASTER
db.driver=/data/vcops/xdb/vcops.bootstrap
```

10 Save and close *persistence.properties*.

11 In the administration interface, bring the replica node online, and verify that it becomes the master node and bring the remaining cluster nodes online.

What to do next

After creating a master replica node, you have the following options.

- New, unstarted clusters:
  - Create and add data nodes.
  - Create and add remote collector nodes.
  - Click **Start vRealize Operations Manager** to start the cluster, and log in to finish configuring the product.

    The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.
- Established, running clusters:
  - Create and add data nodes.
  - Create and add remote collector nodes.

Gathering More Data by Adding a vRealize Operations Manager Remote Collector Node

5

You deploy and configure remote collector nodes so that vRealize Operations Manager can add to its inventory of objects to monitor without increasing the processing load on vRealize Operations Manager analytics.

This chapter includes the following topics:

About vRealize Operations Manager Remote Collector Nodes

A remote collector node is an additional cluster node that allows vRealize Operations Manager to gather more objects into its inventory for monitoring. Unlike data nodes, remote collector nodes only include the collector role of vRealize Operations Manager, without storing data or processing any analytics functions.

A remote collector node is usually deployed to navigate firewalls, reduce bandwidth across data centers, connect to remote data sources, or reduce the load on the vRealize Operations Manager analytics cluster.

Remote collectors do not buffer data while the network is experiencing a problem. If the connection between remote collector and analytics cluster is lost, the remote collector does not store data points that occur during that time. In turn, and after the connection is restored, vRealize Operations Manager does not retroactively incorporate associated events from that time into any monitoring or analysis.

You must have at least a master node before adding remote collector nodes.

Run the Setup Wizard to Create a Remote Collector Node

In distributed vRealize Operations Manager environments, remote collector nodes increase the inventory of objects that you can monitor without increasing the load on vRealize Operations Manager in terms of data storage, processing, or analysis.

Prerequisites

- Create nodes by deploying the vRealize Operations Manager vApp.

  During vApp deployment, select a remote collector size option.
- Create and configure the master node.
- Note the fully qualified domain name (FQDN) or IP address of the master node.

Procedure

1 In a Web browser, navigate to the name or IP address of the deployed OVF that will become the remote collector node.

   The setup wizard appears, and you do not need to log in to vRealize Operations Manager.

2 Click **Expand an Existing Installation**.

3 Click **Next**.

4 Enter a name for the node, for example, **`Remote-1`**.

5 From the **Node Type** drop-down menu, select **Remote Collector**.

6 Enter the FQDN or IP address of the master node and click **Validate**.

7 Select **Accept this certificate** and click **Next**.

   If necessary, locate the certificate on the master node and verify the thumbprint.

8 Verify the vRealize Operations Manager administrator username of **`admin`**.

9 Enter the vRealize Operations Manager administrator password.

   Alternatively, instead of a password, type a passphrase that you were given by the vRealize Operations Manager administrator.

10 Click **Next**, and click **Finish**.

   The administration interface appears, and it takes several minutes for vRealize Operations Manager to finish adding the remote collector node.

What to do next

After creating a remote collector node, you have the following options.

- New, unstarted clusters:
  - Create and add data nodes.
  - Create and add more remote collector nodes.
  - Create a high availability master replica node.
  - Click **Start vRealize Operations Manager** to start the cluster, and log in to finish configuring the product.

    The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.
- Established, running clusters:
  - Create and add data nodes.
  - Create and add more remote collector nodes.
  - Create a high availability master replica node, which requires a cluster restart.

Continuing With a New vRealize Operations Manager Installation

6

After you deploy the vRealize Operations Manager nodes and complete the initial setup, you continue with installation by logging in for the first time and configuring a few settings.

This chapter includes the following topics:

About New vRealize Operations Manager Installations

A new vRealize Operations Manager installation requires that you deploy and configure nodes. Then, you add solutions for the kinds of objects to monitor and manage.

After you add solutions, you configure them in the product and add monitoring policies that gather the kind of data that you want.

Logging In for the First Time (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_first_time_login)

Log In and Continue with a New Installation

To finish a new vRealize Operations Manager installation, you log in and complete a one-time process to license the product and configure solutions for the kinds of objects that you want to monitor.

Prerequisites

- Create the new cluster of vRealize Operations Manager nodes.
- Verify that the cluster has enough capacity to monitor your environment. See "Sizing the vRealize Operations Manager Cluster," on page 15.

Procedure

1. In a Web browser, navigate to the IP address or fully qualified domain name of the master node.
2. Enter the username **admin** and the password that you defined when you configured the master node, and click **Login**.

   Because this is the first time you are logging in, the administration interface appears.
3. To start the cluster, click **Start vRealize Operations Manager**.
4. Click **Yes**.

   The cluster might take from 10 to 30 minutes to start, depending on your environment. Do not make changes or perform any actions on cluster nodes while the cluster is starting.

5 When the cluster finishes starting and the product login page appears, enter the admin username and password again, and click **Login**.

A one-time licensing wizard appears.

6 Click **Next**.

7 Read and accept the End User License Agreement, and click **Next**.

8 Enter your product key, or select the option to run vRealize Operations Manager in evaluation mode.

Your level of product license determines what solutions you may install to monitor and manage objects.

- Standard. vCenter only
- Advanced. vCenter plus other infrastructure solutions
- Enterprise. All solutions

vRealize Operations Manager does not license managed objects in the same way that vSphere does, so there is no object count when you license the product.

Note When you transition to the Standard edition, you no longer have the Advanced and Enterprise features. After the transition, delete any content that you created in the other versions to ensure that you comply with EULA and verify the license key which supports the Advanced and Enterprise features.

---

9 If you entered a product key, click **Validate License Key**.

10 Click **Next**.

11 Select whether or not to return usage statistics to VMware, and click **Next**.

12 Click **Finish**.

The one-time wizard finishes, and the vRealize Operations Manager interface appears.

What to do next

- Use the vRealize Operations Manager interface to configure the solutions that are included with the product.
- Use the vRealize Operations Manager interface to add more solutions.
- Use the vRealize Operations Manager interface to add monitoring policies.

Connecting vRealize Operations Manager to Data Sources

7

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:

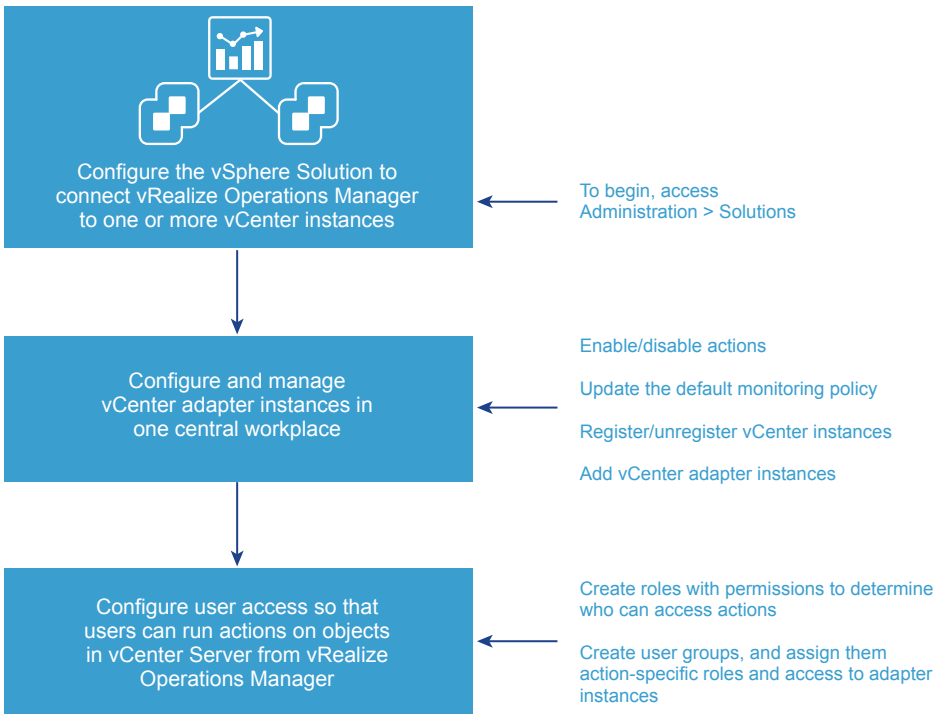
VMware vSphere Solution in vRealize Operations Manager

The VMware vSphere solution connects vRealize Operations Manager to 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. The vSphere solution includes actions that you can run on the vCenter Server from vRealize Operations Manager to manage those objects as you respond to problems and alerts. Actions are run from toolbars in vRealize Operations Manager.

Configuring the vSphere Solution

The vSphere solution is provided with vRealize Operations Manager. It includes the vCenter Server adapter. To configure the vSphere solution, you configure one or more vCenter Server adapter instances, and configure user access so that users can run actions.



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

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.

Add 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)

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**.

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**.

If you want to customize this policy, access the policy in the **Policies** page.

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," on page 46.

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 7-1. 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

Table 7-1. Supported Operating Systems for the Endpoint Operations Management Agent (Continued)

Operating System	Processor Architecture	JVM
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 on page 40

  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 on page 42

  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 on page 43

  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 on page 43

  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 on page 44

  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," on page 71.

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," on page 74.
- 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," on page 46.
- 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	`epops-agent-x86-64-linux-`*`version`*`.rpm`
32bit Operating System	`epops-agent-x86-linux-`*`version`*`.rpm`
No Arch	`epops-agent-noarch-linux-`*`version`*`.rpm`

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," on page 48.

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," on page 74.
- 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	`epops-agent-x86-64-linux-`*`version`*`.tar.gz`
32bit Operating System	`epops-agent-x86-linux-`*`version`*`.tar.gz`
No Arch	`epops-agent-noJRE-`*`version`*`.tar.gz`

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," on page 66.

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," on page 74.
- 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	`epops-agent-x86-64-win-`*`version`*`.zip`
32bit Operating System	`epops-agent-win32-`*`version`*`.zip`
No Arch	`epops-agent-noJRE-`*`version`*`.zip`

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," on page 66.

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," on page 44.

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," on page 74.
- 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	`epops-agent-x86-64-win-`*`version`*`.exe`
32bit Operating System	`epops-agent-x86-win-`*`version`*`.exe`

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," on page 49.

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 7-2. Silent Command Line Installer Parameters

Parameter	Value	Mandatory/Optional	Comments
`–serverAddress`	FQDN/iP address	Mandatory	FQDN or IP address of the vRealize Operations Manager server.
`–username`	string	Mandatory	
`–securePort`	number	Optional	Default is `443`
`–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 7-3. 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 End Point Operations Management agent. For more information , see "Java Prerequisites for the Endpoint Operations Management Agent," on page 45.

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.

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 on page 48

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 on page 49

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

3 Configure an Endpoint Operations Management Agent Keystore on page 50

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 on page 50

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 on page 51

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 on page 51

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
`agent.setup.serverIP`	Specify the address or hostname of the vRealize Operations Manager server.
`agent.setup.serverSSLPort`	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.
`agent.setup.serverLogin`	Specify the user name for the agent to use when connecting to the vRealize Operations Managerserver. If you change the value from the `username` default value, verify that the user account is correctly configured on the vRealize Operations Manager server.
`agent.setup.serverPword`	Specify the password for the agent to use, together with the user name specified in `agent.setup.camLogin`, when connecting to thevRealize 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
`agent.setup.serverCertificateThumbprint`	Provides details about the server certificate to trust. This parameter 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.

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

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

Operating System	Command
Linux	`./bin/ep-agent.sh set-property PropertyKey PropertyValue`
Windows	`./bin/ep-agent.bat set-property PropertyKey PropertyValue`

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	`ep-agent.sh start`
Windows	Install the Windows service for the agent, then run the `it: ep-agent.bat install ep-agent.bat start` command. 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 anEndpoint 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.

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

Prompt	Description
Enter the server hostname or IP address	If the server is on the same machine as the agent, you can enter `localhost`. If a firewall is blocking traffic from the agent to the server, specify the address of the firewall.
Enter the server SSL port	Specify the SSL port on the vRealize Operations Manager server to which the agent must connect. The default port is 443.
The server has presented an untrusted certificate	If this warning appears, but your server is signed by a trusted certificate or you have updated the `thumbprint` property to contain the thumbprint, this agent might be subject to a man-in-the-middle attack. Review the displayed certificate thumbprint details carefully.
Enter your server username	Enter the name of a vRealize Operations Manager user with `agentManager` permissions.
Enter your server password	Enter the password for the specified vRealize Operations Manager. Do not store the password in the `agent.properties` 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 anEndpoint 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
+Dhp7213XQiyvtwI4tMlbGJfZMBPG23KnsUWu3OKrW35gB+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," on page 71.

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 on page 55

  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 on page 55

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

- agent.keystore.path Property on page 55

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

- agent.listenPort Property on page 56

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

- agent.logDir Property on page 56

  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 on page 56

  The path and name of the agent log file.

- agent.logLevel Property on page 56

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

- scheduleThread.queuesize Property on page 65
  Use this property to limit the metric collection queue size (the number of metrics) for a plug-in.
- sigar.mirror.procnet Property on page 66
  `mirror /proc/net/tcp` on Linux.
- sigar.pdh.enableTranslation Property on page 66
  Use this property to enable translation based on the detected locale of the operating system.
- snmpTrapReceiver.listenAddress Property on page 66
  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," on page 55 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," on page 55.

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.unidirectional`.

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.proxyPort` and `agent.setup.unidirectional`.

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 our `hqadmin`.

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.

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.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
```

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

Attribute	Description
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
%user%	The name of the user on whose behalf the event occurred.
%computer%	The name of the computer on which the event occurred.
%source%	The software that logged the Windows event.
%event%	A number identifying the particular event type.
%message%	The event message.
%category%	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_Admistrator@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.procnet 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," on page 69.

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," on page 74.

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
`start`	Starts the agent as a daemon process.
`stop`	Stops the agent's JVM process.
`restart`	Stops and then starts the agent's JVM process.
`status`	Queries the status of the agent's JVM process.
`dump`	Runs a thread dump for the agent process, and writes the result to the `agent.log` file in `AgentHome/log`.
`ping`	Pings the agent process.
`setup`	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
`install`	Installs the agent NT service. You must run `start` after running `install`.
`start`	Starts the agent as an NT service.
`stop`	Stops the agent as an NT service.
`remove`	Removes the agent's service from the NT service table.
`query`	Queries the current status of the agent NT service (status).
`dump`	Runs a thread dump for the agent process, and writes the result to the `agent.log` file in `AgentHome/log`.
`ping`	Pings the agent process.
`setup`	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 thevCenter 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 a 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	1 Run `epops-agent remove`. 2 Remove the agent token and the `data` folder. 3 Run `epops-agent install`. 4 Run `epops-agent start`.

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 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 in 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 on page 70

  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 on page 71

  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 on page 71

  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 on page 71

  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," on page 70.

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," on page 40.

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 on page 72

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

2 Deploy and Start Multiple Agents One-By-One on page 73

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 on page 73

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," on page 71 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," on page 73 or "Deploy and Start Multiple Agents Simultaneously," on page 73.

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," on page 71 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," on page 71 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," on page 72.

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 zxfp $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 zxfp $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.

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.

Administrator	Includes privileges to all features, objects, and actions in vRealize Operations Manager.
ReadOnly	Users have read-only access and can perform read operations, but cannot perform write actions such as create, update, or delete.
PowerUser	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.
PowerUserMinusRemediation	Users have privileges to perform the actions of the Administrator role except for privileges to user management, cluster management, and remediation actions.
ContentAdmin	Users can manage all content, including views, reports, dashboards, and custom groups in vRealize Operations Manager
GeneralUser-1 through GeneralUser-4	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.
AgentManager	Users can deploy and configure Endpoint Operations Management agents.

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	Supply the PTQL query in the form: `Class.Attribute.operator=value`. For example, `Pid.PidFile.eq=/var/run/sshd.pid`. Where: ■ `Class` is the name of the Sigar class without the Proc prefix. ■ `Attribute` is an attribute of the given Class, index into an array or key in a Map class. ■ `operator` is one of the following (for String values): ■ `eq` Equal to value ■ `ne` Not Equal to value ■ `ew` Ends with value ■ `sw` Starts with value ■ `ct` Contains value (substring) ■ `re` Regular expression value matches Delimit queries with a comma.
Windows Service	Monitor an application that runs as a service under Windows. To configure it, you supply its Service Name in Windows. To determine the Service Name: 1 Select **Run** from the Windows Start menu. 2 Type `services.msc` in the run dialog and click **OK**. 3 In the list of services displayed, right-click the service to monitor and choose **Properties**. 4 Locate the Service Name on the **General** tab.
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.

Endpoint Operations Management Agent Upgrade for vRealize Operations Manager 6.3

The Endpoint Operations Management agent for vRealize Operations Manager 6.3 is not backward compatible. vRealize Operations Manager 6.3 works only with the Endpoint Operations Management agent 6.3 and does not work with the previous versions. The Endpoint Operations Management agent 6.3 does not work with previous versions of vRealize Operations Manager.

Upgrade the Endpoint Operations Management agents in the following order:

1 Upgrade Endpoint Operations Management agents 6.2 and above to 6.3.

2 Upgrade vRealize Operations Manager 6.2 and above to vRealize Operations Manager 6.3.

Follow this order to avoid errors during communication with the Endpoint Operations Management agent.

Note You cannot upgrade Endpoint Operations Management agents from 6.1 to 6.3.

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 7-4. 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.

Migrate a vCenter Operations Manager Deployment into this Version

By importing data, an established or production version of vRealize Operations Manager can assume the monitoring of a vCenter Operations Manager deployment.

You cannot migrate vCenter Operations Manager directly to this version of vRealize Operations Manager. Instead, you follow a two-step process:

1 Migrate and import vCenter Operations Manager 5.8.x into vRealize Operations Manager 6.0.x as described in the version 6.0.x documentation.

2 Use the vRealize Operations Manager **Software Update** option to update vRealize Operations Manager 6.0.x to this version.

Note Make sure your vCenter Operations Manager 5.8.x and vRealize Operations Manager 6.0.x instances are on the same physical network. Otherwise the data import may not work.

vRealize Operations Manager Post-Installation Considerations

8

After you install vRealize Operations Manager, there are post-installation tasks that might need your attention.

This chapter includes the following topics:

About Logging In to vRealize Operations Manager

Logging in to vRealize Operations Manager requires that you point a Web browser to the fully qualified domain name (FQDN) or IP address of a node in the vRealize Operations Manager cluster.

When you log in to vRealize Operations Manager, there are a few things to keep in mind.

- After initial configuration, the product interface URL is:

  https://*node-FQDN-or-IP-address*

- Before initial configuration, the product URL opens the administration interface instead.
- After initial configuration, the administration interface URL is:

  https://*node-FQDN-or-IP-address*/admin

- The administrator account name is admin. The account name cannot be changed.
- The admin account is different from the root account used to log in to the console, and does not need to have the same password.
- When logged in to the administration interface, avoid taking the node that you are logged into offline and shutting it down. Otherwise, the interface closes.
- The number of simultaneous login sessions before a performance decrease depends on factors such as the number of nodes in the analytics cluster, the size of those nodes, and the load that each user session expects to put on the system. Heavy users might engage in significant administrative activity, multiple simultaneous dashboards, cluster management tasks, and so on. Light users are more common and often require only one or two dashboards.

  The sizing spreadsheet for your version of vRealize Operations Manager contains further detail about simultaneous login support. See Knowledge Base article 2093783.

- You cannot log in to a vRealize Operations Manager interface with user accounts that are internal to vRealize Operations Manager, such as the maintenanceAdmin account.

- You cannot open the product interface from a remote collector node, but you can open the administration interface.
- For supported Web browsers, see the vRealize Operations Manager Release Notes for your version.

Secure the vRealize Operations Manager Console

After you install vRealize Operations Manager, you secure the console of each node in the cluster by logging in for the first time.

Procedure

1 Locate the node console in vCenter or by direct access. In vCenter, use Alt+F1 to access the login prompt.

For security, vRealize Operations Manager remote terminal sessions are disabled by default.

2 Log in as **root**.

vRealize Operations Manager prevents you from accessing the command prompt until you create a root password.

3 When prompted for a password, press Enter.

4 When prompted for the old password, press Enter.

5 When prompted for the new password, enter the root password that you want, and note it for future reference.

6 Re-enter the root password.

7 Log out of the console.

Log in to a Remote vRealize Operations Manager Console Session

As part of managing or maintaining the nodes in your vRealize Operations Manager cluster, you might need to log in to a vRealize Operations Manager node through a remote console.

For security, remote login is disabled in vRealize Operations Manager by default. To enable remote login, take the following steps.

Procedure

1 Locate the node console in vCenter or by direct access. In vCenter, use Alt+F1 to access the login prompt.

2 Log in as **root**. If this is the first time logging in, you must set a root password.

a When prompted for a password, press Enter.

b When prompted for the old password, press Enter.

c When prompted for the new password, enter the root password that you want, and note it for future reference.

d Re-enter the root password.

3 To enable remote login, enter the following command:

```
service sshd start
```

The Customer Experience Improvement Program

This product participates in VMware's Customer Experience Improvement Program (CEIP). The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. You can choose to join or leave the CEIP for vRealize Operations Manager at any time.

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html .

Join or Leave the Customer Experience Improvement Program for vRealize Operations Manager

You can join or leave the Customer Experience Improvement Program (CEIP) for vRealize Operations Manager at any time.

vRealize Operations Manager gives you the opportunity to join the Customer Experience Improvement Program (CEIP) when you initially install and configure the product. After installation, you can join or leave the CEIP by following these steps.

Procedure

1 In vRealize Operations Manager, click **Administration**.

2 Select **Global Settings**.

3 From the toolbar, click the **Edit** icon.

4 Select or clear the **Customer Experience Improvement Program** option.

When selected, the option activates the Program and sends data to https://vmware.com.

5 Click **OK**.

9 Updating Your Software

You can update your existing vRealize Operations Manager deployments to a newly released version.

When you perform a software update, you need to make sure you use the correct PAK file for your cluster. A good practice is to take a snapshot of the cluster before you update the software, but you must remember to delete the snapshot once the update is complete.

If you have customized the content that vRealize Operations Manager provides such as alerts, symptoms, recommendations, and policies, and you want to install content updates, clone the content before performing the update. In this way, you can select the option to reset out-of-the-box content when you install the software update, and the update can provide new content without overwriting customized content.

This chapter includes the following topics:

Obtain the Software Update PAK File

Each type of cluster update requires a specific PAK file. Make sure you are using the correct one.

Download the Correct PAK files

To update your vRealize Operations Manager environment, you need to download the right PAK file for the clusters you wish to upgrade. Notice that only the Virtual Appliance clusters use an OS Update PAK file. Host name entries in the `/etc/hosts` of each node might be reset when applying the OS update PAK file for an update from vRealize Operations 6.0.x to version 6.1. You can manually update the hosts file after completing the software update.

Table 9-1. Specific PAK Files for Different Cluster Types

Cluster Type	OS Update	Product Update
Virtual Appliance clusters. Use both the OS and the product update PAK files.	`vRealize_Operations_Manager-VA-OS-xxx.pak`	`vRealize_Operations_Manager-VA-xxx.pak`
Virtual Appliance heterogeneous clusters. Use both the OS and the product update PAK files.	`vRealize_Operations_Manager-VA-OS-xxx.pak`	`vRealize_Operations_Manager-VA-WIN-xxx.pak`
RHEL standalone clusters.		`vRealize_Operations_Manager-RHEL-xxx.pak`

Table 9-1. Specific PAK Files for Different Cluster Types (Continued)

Cluster Type	OS Update	Product Update
RHEL heterogeneous clusters. Use this file if you have a heterogeneous cluster that has RHEL nodes and Windows Remote Collectors.		`vRealize_Operations_Manager-RHEL-WIN-xxx.pak`
Windows clusters		`vRealize_Operations_Manager-WIN-xxx.pak`

Create a Snapshot as Part of an Update

It's a good practice to create a snapshot of each node in a cluster before you update a vRealize Operations Manager cluster. Once the update is complete, you must delete the snapshot to avoid performance degradation.

For more information about snapshots, see the vSphere Virtual Machine Administration documentation.

Procedure

1 Log into the vRealize Operations Manager Administrator interface at `https://<master-node-FQDN-or-IP-address>/admin`.

2 Select a node in the cluster.

3 Click **Take Offline**.

Repeat for each node.

4 When all nodes are offline, open the vSphere client.

5 Right-click a vRealize Operations Manager virtual machine.

6 Click **Snapshot** and then click **Take Snapshot**.

a Name the snapshot. Use a meaningful name such as "Pre-Update."

b Uncheck the **Snapshot the Virtual Machine Memory** check box.

c Uncheck the **Ensure Quiesce Guest File System (Needs VMware Tools installed)** check box.

d Click **OK**.

7 Repeat these steps for each node in the cluster.

What to do next

Start the update process as described in "Install a Software Update," on page 86.

Install a Software Update

If you have already installed vRealize Operations Manager, you can update your software when a newer version becomes available.

Note Installation might take several minutes or even a couple hours depending on the size and type of your clusters and nodes.

Prerequisites

- Create a snapshot of each node in your cluster. For information about how to perform this task, see the vRealize Operations Manager Information Center.

- Obtain the PAK file for your cluster. For information about which file to use, see the vRealize Operations Manager Information Center.
- 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**.
- The version 6.2.1 vRealize Operations Manager update operation has a validation process that identifies issues before you start to update your software. Although it is good practice to run the pre-update check and resolve any issues found, users who have environmental constraints can disable this validation check.

  To disable the pre-update validation check, perform the following steps:

  - Edit the update file to`/storage/db/pakRepoLocal/bypass_prechecks_vRealizeOperationsManagerEnterprise-buildnumberofupdate.json`.
  - Change the value to TRUE and run the update.

  Note If you disable the validation, you might encounter blocking failures during the update itself.

Procedure

1. Log into the master node vRealize Operations Manager Administrator interface of your cluster at `https://master-node-FQDN-or-IP-address/admin`.
2. Click **Software Update** in the left panel.
3. Click **Install a Software Update** in the main panel.
4. Follow the steps in the wizard to locate and install your PAK file.
   a. If you are updating a Virtual Appliance deployment, perform the OS update.

      This updates the OS on the virtual appliance and restarts each virtual machine.

   b. Install the product update PAK file.

      Wait for the software update to complete. When it does, the Administrator interface logs you out.
5. Log back into the master node Administrator interface.

   The main Cluster Status page appears and cluster goes online automatically. The status page also displays the Bring Online button, but do not click it.
6. If the browser page does not refresh automatically, refresh the page.

   The cluster status changes to Going Online. When the cluster status changes to Online, the upgrade is complete.

   Note If a cluster fails and the status changes to offline during the installation process of a PAK file update then some nodes become unavailable. To fix this, you can access the Administrator interface and manually take the cluster offline and click **Finish Installation** to continue the installation process.
7. Click **Software Update** to check that the update is done.

   A message indicating that the update completed successfully appears in the main pane.

What to do next

Delete the snapshots you made before the software update.

Note Multiple snapshots can degrade performance, so delete your pre-update snapshots after the software update completes.

Index

R

S

U

V

W