



Red Hat Virtualization 4.3

Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Red Hat Virtualization 4.3 Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Red Hat Virtualization Documentation Team

Red Hat Customer Content Services

rhev-docs@redhat.com

Legal Notice

Copyright © 2019 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

A comprehensive guide to upgrading and updating components in a Red Hat Virtualization environment.

Table of Contents

CHAPTER 1. RED HAT VIRTUALIZATION UPGRADE OVERVIEW	5
PART I. UPGRADING A LOCAL DATABASE ENVIRONMENT	7
CHAPTER 2. UPGRADING FROM 4.0 TO RED HAT VIRTUALIZATION 4.3	8
2.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER	9
2.2. UPGRADING THE MANAGER FROM 4.0 TO 4.1	10
2.3. UPGRADING THE MANAGER FROM 4.1 TO 4.2	10
2.4. UPDATING INDIVIDUAL HOSTS	11
2.5. CHANGING THE CLUSTER COMPATIBILITY VERSION	13
2.6. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	13
2.7. CHANGING THE DATA CENTER COMPATIBILITY VERSION	14
2.8. UPGRADING THE MANAGER FROM 4.2 TO 4.3	15
2.9. CHANGING THE CLUSTER COMPATIBILITY VERSION	16
2.10. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	16
2.11. CHANGING THE DATA CENTER COMPATIBILITY VERSION	17
2.12. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	17
CHAPTER 3. UPGRADING FROM 4.1 TO RED HAT VIRTUALIZATION 4.3	21
3.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER	21
3.2. UPGRADING THE MANAGER FROM 4.1 TO 4.2	22
3.3. UPGRADING THE MANAGER FROM 4.2 TO 4.3	23
3.4. UPDATING ALL HOSTS IN A CLUSTER	24
3.5. CHANGING THE CLUSTER COMPATIBILITY VERSION	26
3.6. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	26
3.7. CHANGING THE DATA CENTER COMPATIBILITY VERSION	27
3.8. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	27
3.9. UPDATING OVN PROVIDERS INSTALLED IN RED HAT VIRTUALIZATION 4.1	30
CHAPTER 4. UPGRADING FROM 4.2 TO RED HAT VIRTUALIZATION 4.3	31
4.1. ANALYZING THE ENVIRONMENT	31
4.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER	32
4.3. UPGRADING THE MANAGER FROM 4.2 TO 4.3	33
4.4. UPDATING ALL HOSTS IN A CLUSTER	34
4.5. CHANGING THE CLUSTER COMPATIBILITY VERSION	35
4.6. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	36
4.7. CHANGING THE DATA CENTER COMPATIBILITY VERSION	36
4.8. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	37
PART II. UPGRADING A REMOTE DATABASE ENVIRONMENT	41
CHAPTER 5. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.0 TO RED HAT VIRTUALIZATION 4.3	42
5.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER	43
5.2. UPGRADING THE MANAGER FROM 4.0 TO 4.1	44
5.3. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.2 TO 9.5	45
5.4. UPGRADING THE MANAGER FROM 4.1 TO 4.2	46
5.5. UPDATING INDIVIDUAL HOSTS	47
5.6. CHANGING THE CLUSTER COMPATIBILITY VERSION	49
5.7. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	49
5.8. CHANGING THE DATA CENTER COMPATIBILITY VERSION	50
5.9. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10	50
5.10. UPGRADING THE MANAGER FROM 4.2 TO 4.3	52

5.11. CHANGING THE CLUSTER COMPATIBILITY VERSION	53
5.12. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	53
5.13. CHANGING THE DATA CENTER COMPATIBILITY VERSION	54
5.14. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	55
CHAPTER 6. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.1 TO RED HAT VIRTUALIZATION	
4.3	58
6.1. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.2 TO 9.5	58
6.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER	60
6.3. UPGRADING THE MANAGER FROM 4.1 TO 4.2	61
6.4. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10	62
6.5. UPGRADING THE MANAGER FROM 4.2 TO 4.3	64
6.6. UPDATING ALL HOSTS IN A CLUSTER	65
6.7. CHANGING THE CLUSTER COMPATIBILITY VERSION	66
6.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	67
6.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION	67
6.10. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	68
6.11. UPDATING OVN PROVIDERS INSTALLED IN RED HAT VIRTUALIZATION 4.1	70
CHAPTER 7. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.2 TO RED HAT VIRTUALIZATION	
4.3	72
7.1. ANALYZING THE ENVIRONMENT	72
7.2. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10	73
7.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER	74
7.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3	75
7.5. UPDATING ALL HOSTS IN A CLUSTER	76
7.6. CHANGING THE CLUSTER COMPATIBILITY VERSION	78
7.7. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	78
7.8. CHANGING THE DATA CENTER COMPATIBILITY VERSION	79
7.9. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	80
PART III. UPGRADING A SELF-HOSTED ENGINE ENVIRONMENT	83
CHAPTER 8. UPGRADING A SELF-HOSTED ENGINE FROM 4.0 TO RED HAT VIRTUALIZATION 4.3	84
8.1. ENABLING GLOBAL MAINTENANCE MODE	85
8.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER	85
8.3. UPGRADING THE MANAGER FROM 4.0 TO 4.1	86
8.4. UPGRADING THE MANAGER FROM 4.1 TO 4.2	87
8.5. DISABLING GLOBAL MAINTENANCE MODE	88
8.6. UPDATING INDIVIDUAL HOSTS	89
8.7. CHANGING THE CLUSTER COMPATIBILITY VERSION	90
8.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	91
8.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION	91
8.10. ENABLING GLOBAL MAINTENANCE MODE	92
8.11. UPGRADING THE MANAGER FROM 4.2 TO 4.3	92
8.12. DISABLING GLOBAL MAINTENANCE MODE	93
8.13. CHANGING THE CLUSTER COMPATIBILITY VERSION	94
8.14. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	94
8.15. CHANGING THE DATA CENTER COMPATIBILITY VERSION	95
8.16. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	95
CHAPTER 9. UPGRADING A SELF-HOSTED ENGINE FROM 4.1 TO RED HAT VIRTUALIZATION 4.3	99
9.1. ENABLING GLOBAL MAINTENANCE MODE	99
9.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER	100

9.3. UPGRADING THE MANAGER FROM 4.1 TO 4.2	101
9.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3	102
9.5. DISABLING GLOBAL MAINTENANCE MODE	103
9.6. UPDATING ALL HOSTS IN A CLUSTER	103
9.7. CHANGING THE CLUSTER COMPATIBILITY VERSION	105
9.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	105
9.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION	106
9.10. UPDATING OVN PROVIDERS INSTALLED IN RED HAT VIRTUALIZATION 4.1	106
9.11. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	107
CHAPTER 10. UPGRADING A SELF-HOSTED ENGINE FROM 4.2 TO RED HAT VIRTUALIZATION 4.3	111
10.1. ANALYZING THE ENVIRONMENT	111
10.2. ENABLING GLOBAL MAINTENANCE MODE	112
10.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER	112
10.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3	113
10.5. DISABLING GLOBAL MAINTENANCE MODE	114
10.6. UPDATING ALL HOSTS IN A CLUSTER	115
10.7. CHANGING THE CLUSTER COMPATIBILITY VERSION	116
10.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	117
10.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION	117
10.10. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	118
PART IV. APPENDICES	122
APPENDIX A. UPDATES BETWEEN MINOR RELEASES	123
A.1. ANALYZING THE ENVIRONMENT	123
A.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER	123
A.3. UPDATING A SELF-HOSTED ENGINE	124
A.4. UPDATING ALL HOSTS IN A CLUSTER	126
A.5. UPDATING INDIVIDUAL HOSTS	128
A.6. MANUALLY UPDATING HOSTS	129
APPENDIX B. UPDATING THE LOCAL REPOSITORY FOR AN OFFLINE RED HAT VIRTUALIZATION MANAGER INSTALLATION	131
APPENDIX C. UPGRADING TO RED HAT VIRTUALIZATION MANAGER 4.3 WITH OVIRT-FAST-FORWARD-UPGRADE	132

CHAPTER 1. RED HAT VIRTUALIZATION UPGRADE OVERVIEW

This guide explains how to upgrade your current environment to Red Hat Virtualization 4.3.

Three upgrade paths are documented here:

- **Local database:** Both the Data Warehouse database and the Manager database are installed on the Manager.
- **Remote database:** Either the Data Warehouse database or the Manager database, or both, are on a separate machine.
- **Self-hosted engine:** The Manager is a self-hosted engine.



IMPORTANT

Plan any necessary downtime in advance. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended VMs as soon as possible to apply the configuration changes.

Select the appropriate instructions for your environment from the following table. If your Manager and host versions differ (if you have previously upgraded the Manager but not the hosts), follow the instructions that match the Manager's version.

Table 1.1. Supported Upgrade Paths

Current Manager version	Target Manager version	Relevant section
4.0	4.3	<p>Local database environment: Chapter 2, Upgrading from 4.0 to Red Hat Virtualization 4.3</p> <p>Remote database environment: Chapter 5, Upgrading a Remote Database Environment from 4.0 to Red Hat Virtualization 4.3</p> <p>Self-hosted engine environment: Chapter 8, Upgrading a Self-Hosted Engine from 4.0 to Red Hat Virtualization 4.3</p>
4.1	4.3	<p>Local database environment: Chapter 3, Upgrading from 4.1 to Red Hat Virtualization 4.3</p> <p>Remote database environment: Chapter 6, Upgrading a Remote Database Environment from 4.1 to Red Hat Virtualization 4.3</p> <p>Self-hosted engine environment: Chapter 9, Upgrading a Self-Hosted Engine from 4.1 to Red Hat Virtualization 4.3</p>

Current Manager version	Target Manager version	Relevant section
4.2	4.3	Local database environment: Chapter 4, Upgrading from 4.2 to Red Hat Virtualization 4.3 Remote database environment: Chapter 7, Upgrading a Remote Database Environment from 4.2 to Red Hat Virtualization 4.3 Self-hosted engine environment: Chapter 10, Upgrading a Self-Hosted Engine from 4.2 to Red Hat Virtualization 4.3
4.3.x	4.3.y	Appendix A, Updates between Minor Releases

For interactive upgrade instructions, you can also use the RHV Upgrade Helper available at <https://access.redhat.com/labs/rhvupgradehelper/>. This application asks you to provide information about your upgrade path and your current environment, and presents the relevant steps for upgrade as well as steps to prevent known issues specific to your upgrade scenario.

PART I. UPGRADING A LOCAL DATABASE ENVIRONMENT

CHAPTER 2. UPGRADING FROM 4.0 TO RED HAT VIRTUALIZATION 4.3

The 4.0 compatibility version is not supported after Red Hat Virtualization 4.2. Therefore, when upgrading from Red Hat Virtualization 4.0 you must update the cluster and data center compatibility versions to at least 4.1 before upgrading the Manager from 4.2 to 4.3, then update the compatibility versions again after completing the Manager upgrades.

You must also update the hosts before updating the compatibility versions, but only need to do so once. The host repositories stay the same across Red Hat Virtualization versions, so the hosts will already be upgraded to the latest version after a single update.

Upgrading your environment from 4.0 to 4.3 involves the following steps:

1. [Update the 4.0 Manager to the latest version of 4.0](#)
2. [Upgrade the Manager from 4.0 to 4.1](#)
3. [Upgrade the Manager from 4.1 to 4.2](#)
4. [Update the hosts](#)
5. [Update the compatibility version of the clusters to 4.2](#)
6. [Reboot any running or suspended virtual machines to update their configuration to 4.2](#)
7. [Update the compatibility version of the data centers to 4.2](#)
8. [Upgrade the Manager from 4.2 to 4.3](#)
9. [Update the compatibility version of the cluster to the latest version](#)
10. [Reboot any running or suspended virtual machines to update their configuration to the latest version](#)
11. [Update the compatibility version of the data centers to the latest version](#)
12. [Replace SHA-1 certificates with SHA-256 certificates](#)

Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Subscribing to the Required Entitlements](#) for Red Hat Virtualization 4.0.

2.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

5. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

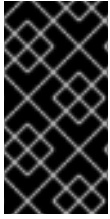


IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

2.2. UPGRADING THE MANAGER FROM 4.0 TO 4.1

Upgrade the Red Hat Virtualization Manager from 4.0 to 4.1.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.1 repositories:

```
# subscription-manager repos \  
--enable=rhel-7-server-rhv-4.1-rpms \  
--enable=rhel-7-server-rhv-4-tools-rpms \  
--enable=jb-eap-7.1-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

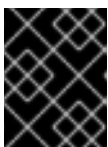
```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.0 repositories to ensure the system does not use any 4.0 packages:

```
# subscription-manager repos \  
--disable=rhel-7-server-rhv-4.0-rpms \  
--disable=jb-eap-7-for-rhel-7-server-rpms \  
--disable=jb-eap-7.0-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

2.3. UPGRADING THE MANAGER FROM 4.1 TO 4.2

Upgrade the Red Hat Virtualization Manager from 4.1 to 4.2.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.2 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.2-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=jb-eap-7-for-rhel-7-server-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.1 repositories to ensure the system does not use any 4.1 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.1-rpms \
  --disable=rhel-7-server-rhv-4.1-manager-rpms \
  --disable=rhel-7-server-rhv-4-tools-rpms \
  --disable=jb-eap-7.0-for-rhel-7-server-rpms \
  --disable=jb-eap-7.1-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You must now update the hosts before you can update the cluster and data center compatibility versions.

2.4. UPDATING INDIVIDUAL HOSTS

Use the host upgrade manager to update individual hosts directly from the Administration Portal.



NOTE

The upgrade manager only checks hosts with a status of **Up** or **Non-operational**, but not **Maintenance**.


Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure

1. Ensure that the correct repositories are enabled. To view a list of currently enabled repositories, run **yum repolist**.
 - For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhel-7-server-rhvh-4-rpms
```
 - For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```
2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Installation** → **Check for Upgrade** and click **OK**.
Open the **Notification Drawer** () and expand the **Events** section to see the result.
4. If an update is available, click **Installation** → **Upgrade**.
5. Click **OK** to update the host. Running virtual machines are migrated according to their migration policy. If migration is disabled for any virtual machines, you are prompted to shut them down. The details of the host are updated in **Compute** → **Hosts** and the status transitions through these stages:

- **Maintenance**
- **Installing**
- **Reboot**
- **Up**

If any virtual machines were migrated off the host, they are now migrated back.



NOTE

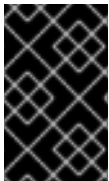
If the update fails, the host's status changes to **Install Failed**. From **Install Failed** you can click **Installation** → **Upgrade** again.

Repeat this procedure for each host in the Red Hat Virtualization environment.

You can now change the cluster compatibility version to 4.2.

2.5. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

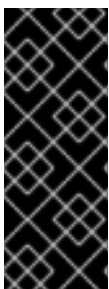


IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.




IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

2.6. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all

running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute → Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



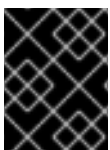
NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now change the data center compatibility version to 4.2.

2.7. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute → Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

2.8. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms \
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms \
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now change the cluster compatibility version to 4.3.

2.9. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

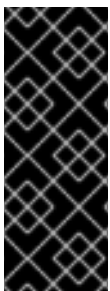


IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

2.10. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now change the data center compatibility version to 4.3.

2.11. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

2.12. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.
- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates](#).

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.

2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\); \1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

5. Restart the **httpd** service:

```
# systemctl restart httpd
```

6. Connect to the Administration Portal to confirm that the warning no longer appears.
7. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\); \1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

7. Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
```

```
# systemctl restart ovirt-imageio-proxy
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **`http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute → Hosts**.
 - b. Select the host and click **Management → Maintenance**.
 - c. Once the host is in maintenance mode, click **Installation → Enroll Certificate**.
 - d. Click **Management → Activate**.

CHAPTER 3. UPGRADING FROM 4.1 TO RED HAT VIRTUALIZATION 4.3

Upgrading your environment from 4.1 to 4.3 involves the following steps:

1. [Update the 4.1 Manager to the latest version of 4.1](#)
2. [Upgrade the Manager from 4.1 to 4.2](#)
3. [Upgrade the Manager from 4.2 to 4.3](#)
4. [Update the hosts](#)
5. [Update the compatibility version of the clusters](#)
6. [Reboot any running or suspended virtual machines to update their configuration](#)
7. [Update the compatibility version of the data centers](#)
8. [Replace SHA-1 certificates with SHA-256 certificates](#)
9. If you installed the technology preview version of Open Virtual Network (OVN) in 4.1, [update the OVN provider's networking plugin](#)

Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Subscribing to the Required Entitlements](#) for Red Hat Virtualization 4.1.

3.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt*setup*
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

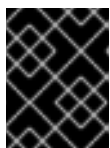


IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

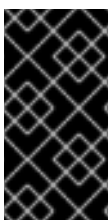


IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

3.2. UPGRADING THE MANAGER FROM 4.1 TO 4.2

Upgrade the Red Hat Virtualization Manager from 4.1 to 4.2.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.2 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.2-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=jb-eap-7-for-rhel-7-server-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.1 repositories to ensure the system does not use any 4.1 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.1-rpms \
  --disable=rhel-7-server-rhv-4.1-manager-rpms \
  --disable=rhel-7-server-rhv-4-tools-rpms \
  --disable=jb-eap-7.0-for-rhel-7-server-rpms \
  --disable=jb-eap-7.1-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

3.3. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.

2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
--enable=rhel-7-server-rhv-4.3-manager-rpms \
--enable=jb-eap-7.2-for-rhel-7-server-rpms \
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
--disable=rhel-7-server-rhv-4.2-manager-rpms \
--disable=jb-eap-7-for-rhel-7-server-rpms \
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now update the hosts.

3.4. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md> for more information about the Ansible role used to automate the updates.

Red Hat recommends updating one cluster at a time.


Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.

- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
6. Review the summary of the hosts and virtual machines that will be affected.
7. Click **Upgrade**.

You can track the progress of host updates in the **Compute → Hosts** view, and in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

3.5. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute → Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

3.6. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

3.7. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

3.8. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates.](#)

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

5. Restart the **httpd** service:

```
# systemctl restart httpd
```

6. Connect to the Administration Portal to confirm that the warning no longer appears.
7. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **http://*your-manager-fqdn*/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+%Y%m%d%H%M%S)"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

-
- 7. Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio-proxy
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **`http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute → Hosts**.
 - b. Select the host and click **Management → Maintenance**.
 - c. Once the host is in maintenance mode, click **Installation → Enroll Certificate**.
 - d. Click **Management → Activate**.

3.9. UPDATING OVN PROVIDERS INSTALLED IN RED HAT VIRTUALIZATION 4.1

If you installed an Open Virtual Network (OVN) provider in Red Hat Virtualization 4.1, you must manually edit its configuration for Red Hat Virtualization 4.2.

Procedure

1. Click **Administration → Providers** and select the OVN provider.
2. Click **Edit**.
3. Click the **Networking Plugin** text field and select **oVirt Network Provider for OVN** from the drop-down list.
4. Click **OK**.

CHAPTER 4. UPGRADING FROM 4.2 TO RED HAT VIRTUALIZATION 4.3

Upgrading your environment from 4.2 to 4.3 involves the following steps:

1. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade](#)
2. [Update the 4.2 Manager to the latest version of 4.2](#)
3. [Upgrade the Manager from 4.2 to 4.3](#)
4. [Update the hosts](#)
5. [Update the compatibility version of the clusters](#)
6. [Reboot any running or suspended virtual machines to update their configuration](#)
7. [Update the compatibility version of the data centers](#)
8. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

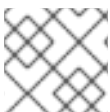
Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2.

4.1. ANALYZING THE ENVIRONMENT

Red Hat recommends running the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyses your environment and displays any known issues that may prevent you from performing an update and suggests how to resolve the issue.

The tool gathers detailed information about your system and presents it as an HTML file.



NOTE

The Log Collection Analysis tool is available from Red Hat Virtualization 4.2.5.

Procedure

1. Install the Log Collection Analysis tool on the Manager:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

4.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

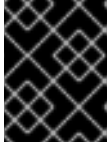
When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

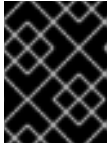
The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

5. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

4.3. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms \
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

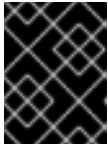
```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
--disable=rhel-7-server-rhv-4.2-manager-rpms \
--disable=jb-eap-7-for-rhel-7-server-rpms \
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now update the hosts.

4.4. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md> for more information about the Ansible role used to automate the updates.

Red Hat recommends updating one cluster at a time.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster,


and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.

- **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
- **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
- **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
- **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.

5. Click **Next**.

6. Review the summary of the hosts and virtual machines that will be affected.

7. Click **Upgrade**.

You can track the progress of host updates in the **Compute → Hosts** view, and in the **Events** section of the **Notification Drawer** () .

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

4.5. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure

1. In the Administration Portal, click **Compute → Clusters**.


2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

4.6. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.

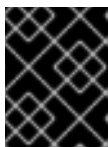


NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

4.7. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

4.8. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.
- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates](#).

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

5. Restart the **httpd** service:

```
# systemctl restart httpd
```

6. Connect to the Administration Portal to confirm that the warning no longer appears.
7. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S)"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
    )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

7. Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio-proxy
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute → Hosts**.

- b. Select the host and click **Management** → **Maintenance**.
- c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
- d. Click **Management** → **Activate**.

PART II. UPGRADING A REMOTE DATABASE ENVIRONMENT

CHAPTER 5. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.0 TO RED HAT VIRTUALIZATION 4.3

The 4.0 compatibility version is not supported after Red Hat Virtualization 4.2. Therefore, when upgrading from Red Hat Virtualization 4.0 you must update the cluster and data center compatibility versions to at least 4.1 before upgrading the Manager from 4.2 to 4.3, then update the compatibility versions again after completing the Manager upgrades.

You must also update the hosts before updating the compatibility versions, but only need to do so once. The host repositories stay the same across Red Hat Virtualization versions, so the hosts will already be upgraded to the latest version after a single update.

Upgrading your environment from 4.0 to 4.3 involves the following steps:

1. [Update the 4.0 Manager to the latest version of 4.0](#)
2. [Upgrade the Manager from 4.0 to 4.1](#)
3. [Upgrade the database from PostgreSQL 9.2 to 9.5](#)
4. [Upgrade the Manager from 4.1 to 4.2](#)
5. [Update the hosts](#)
6. [Update the compatibility version of the clusters to 4.2](#)
7. [Update the compatibility version of the data centers to 4.2](#)
8. [Reboot any running or suspended virtual machines to update their configuration to 4.2](#)
9. [Upgrade the database from PostgreSQL 9.5 to 10.0](#)
10. [Upgrade the Manager from 4.2 to 4.3](#)
11. [Update the compatibility version of the clusters to the latest version](#)
12. [Reboot any running or suspended virtual machines to update their configuration to the latest version](#)
13. [Update the compatibility version of the data centers to the latest version](#)
14. [Replace SHA-1 certificates with SHA-256 certificates](#)

Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Subscribing to the Required Entitlements](#) for Red Hat Virtualization 4.0.

5.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

5. Update the base operating system and any optional packages installed on the Manager:

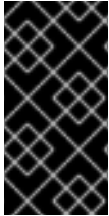
```
# yum update
```

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

5.2. UPGRADING THE MANAGER FROM 4.0 TO 4.1

Upgrade the Red Hat Virtualization Manager from 4.0 to 4.1.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.1 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.1-rpms \
  --enable=rhel-7-server-rhv-4-tools-rpms \
  --enable=jb-eap-7.1-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

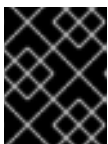
```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.0 repositories to ensure the system does not use any 4.0 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.0-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms \
  --disable=jb-eap-7.0-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the upgrade.

5.3. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.2 TO 9.5

Red Hat Virtualization 4.2 uses PostgreSQL 9.5 instead of PostgreSQL 9.2. If your databases are installed locally, the upgrade script will automatically upgrade them from version 9.2 to 9.5. However, if either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

1. Stop the service running on the machine:

- Stop the **ovirt-engine** service on the Manager machine:

```
# systemctl stop ovirt-engine
```

- Stop the **ovirt-engine-dwh** service on the Data Warehouse machine:

```
# systemctl stop ovirt-engine-dwhd
```

2. Enable the required repository to receive the PostgreSQL 9.5 package:
Enable either the Red Hat Virtualization Manager repository:

```
# subscription-manager repos --enable=rhel-7-server-rhv-4.2-manager-rpms
```

or the SCL repository:

```
# subscription-manager repos --enable rhel-server-rhscl-7-rpms
```

3. Install the PostgreSQL 9.5 packages:

```
# yum install rh-postgresql95 rh-postgresql95-postgresql-contrib
```

4. Stop and disable the PostgreSQL 9.2 service:

```
# systemctl stop postgresql
# systemctl disable postgresql
```

5. Upgrade the PostgreSQL 9.2 database to PostgreSQL 9.5:

```
# scl enable rh-postgresql95 -- postgresql-setup upgrade
```

6. Start and enable the **rh-postgresql95-postgresql.service** and check that it is running:

```
# systemctl start rh-postgresql95-postgresql.service
# systemctl enable rh-postgresql95-postgresql.service
# systemctl status rh-postgresql95-postgresql.service
```

Ensure that you see an output similar to the following:

```
rh-postgresql95-postgresql.service - PostgreSQL database server
Loaded: loaded (/usr/lib/systemd/system/rh-postgresql95-postgresql.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2018-05-07 08:48:27 CEST; 1h 59min ago
```

7. Log in to the database and enable the **uuid-oss** extension:

```
# su - postgres -c "scl enable rh-postgresql95 -- psql -d database-name"
```

8. Execute the following SQL commands:

```
# database-name=# DROP FUNCTION IF EXISTS uuid_generate_v1();
# database-name=# CREATE EXTENSION "uuid-oss";
```

9. Copy the **pg_hba.conf** client configuration file from the 9.2 environment to your 9.5 environment:

```
# cp -p /var/lib/pgsql/data/pg_hba.conf /var/opt/rh/rh-postgresql95/lib/pgsql/data/pg_hba.conf
```

10. Update the following parameters in **/var/opt/rh/rh-postgresql95/lib/pgsql/data/postgresql.conf**:

```
listen_addresses='*'
autovacuum_vacuum_scale_factor = 0.01
autovacuum_analyze_scale_factor = 0.075
autovacuum_max_workers = 6
maintenance_work_mem = 65536
max_connections = 150
work_mem = 8192
```

11. Restart the PostgreSQL 9.5 service to apply the configuration changes:

```
# systemctl restart rh-postgresql95-postgresql.service
```

12. Start the **ovirt-engine-dwhd** service:

```
# systemctl start ovirt-engine-dwhd
```

You can now upgrade the Manager to 4.2.

5.4. UPGRADING THE MANAGER FROM 4.1 TO 4.2

Upgrade the Red Hat Virtualization Manager from 4.1 to 4.2.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.2 repositories:

```
# subscription-manager repos \
--enable=rhel-7-server-rhv-4.2-manager-rpms \
--enable=rhel-7-server-rhv-4-manager-tools-rpms \
--enable=jb-eap-7-for-rhel-7-server-rpms \
--enable=rhel-7-server-ansible-2-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt-*setup*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.1 repositories to ensure the system does not use any 4.1 packages:

```
# subscription-manager repos \
--disable=rhel-7-server-rhv-4.1-rpms \
--disable=rhel-7-server-rhv-4.1-manager-rpms \
--disable=rhel-7-server-rhv-4-tools-rpms \
--disable=jb-eap-7.0-for-rhel-7-server-rpms \
--disable=jb-eap-7.1-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You must now update the hosts before you can update the cluster and data center compatibility versions.

5.5. UPDATING INDIVIDUAL HOSTS

Use the host upgrade manager to update individual hosts directly from the Administration Portal.



NOTE

The upgrade manager only checks hosts with a status of **Up** or **Non-operational**, but not **Maintenance**.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.

- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure


1. Ensure that the correct repositories are enabled. To view a list of currently enabled repositories, run **yum repolist**.

- For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhel-7-server-rhvh-4-rpms
```

- For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
--enable=rhel-7-server-rpms \
--enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
--enable=rhel-7-server-ansible-2-rpms
```

2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Installation** → **Check for Upgrade** and click **OK**.
Open the **Notification Drawer** () and expand the **Events** section to see the result.
4. If an update is available, click **Installation** → **Upgrade**.
5. Click **OK** to update the host. Running virtual machines are migrated according to their migration policy. If migration is disabled for any virtual machines, you are prompted to shut them down. The details of the host are updated in **Compute** → **Hosts** and the status transitions through these stages:
 - **Maintenance**
 - **Installing**
 - **Reboot**
 - **Up**
If any virtual machines were migrated off the host, they are now migrated back.

**NOTE**

If the update fails, the host's status changes to **Install Failed**. From **Install Failed** you can click **Installation** → **Upgrade** again.

Repeat this procedure for each host in the Red Hat Virtualization environment.

You can now change the cluster compatibility version to 4.2.

5.6. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

**IMPORTANT**

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.


Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

**IMPORTANT**

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

5.7. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now change the data center compatibility version to 4.2.

5.8. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

5.9. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10

Red Hat Virtualization 4.3 uses PostgreSQL 10 instead of PostgreSQL 9.5. If your databases are installed locally, the upgrade script automatically upgrades them from version 9.5 to 10. However, if either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

1. Stop the service running on the machine:
 - Stop the **ovirt-engine** service on the Manager machine:

-

```
# systemctl stop ovirt-engine
```

- Stop the **ovirt-engine-dwh** service on the Data Warehouse machine:

```
# systemctl stop ovirt-engine-dwhd
```

2. Enable the required repository to receive the PostgreSQL 10 package:
Enable either the Red Hat Virtualization Manager repository:

```
# subscription-manager repos --enable=rhel-7-server-rhv-4.3-manager-rpms
```

or the SCL repository:

```
# subscription-manager repos --enable rhel-server-rhscl-7-rpms
```

3. Install the PostgreSQL 10 packages:

```
# yum install rh-postgresql10 rh-postgresql10-postgresql-contrib
```

4. Stop and disable the PostgreSQL 9.5 service:

```
# systemctl stop rh-postgresql95-postgresql
# systemctl disable rh-postgresql95-postgresql
```

5. Upgrade the PostgreSQL 9.5 database to PostgreSQL 10:

```
# scl enable rh-postgresql10 -- postgresql-setup --upgrade-from=rh-postgresql95-postgresql
--upgrade
```

6. Start and enable the **rh-postgresql10-postgresql.service** and check that it is running:

```
# systemctl start rh-postgresql10-postgresql.service
# systemctl enable rh-postgresql10-postgresql.service
# systemctl status rh-postgresql10-postgresql.service
```

Ensure that you see output similar to the following:

```
rh-postgresql10-postgresql.service - PostgreSQL database server
Loaded: loaded (/usr/lib/systemd/system/rh-postgresql10-postgresql.service;
enabled; vendor preset: disabled)
Active: active (running) since ...
```

7. Copy the **pg_hba.conf** client configuration file from the PostgreSQL 9.5 environment to the PostgreSQL 10 environment:

```
# cp -p /var/opt/rh/rh-postgresql95/lib/pgsql/data/pg_hba.conf /var/opt/rh/rh-
postgresql10/lib/pgsql/data/pg_hba.conf
```

8. Update the following parameters in **/var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf**:

```
listen_addresses='*'
autovacuum_vacuum_scale_factor=0.01
autovacuum_analyze_scale_factor=0.075
autovacuum_max_workers=6
maintenance_work_mem=65536
max_connections=150
work_mem = 8192
```

- Restart the PostgreSQL 10 service to apply the configuration changes:

```
# systemctl restart rh-postgresql10-postgresql.service
```

- Start the **ovirt-engine-dwhd** service:

```
# systemctl start ovirt-engine-dwhd
```

You can now upgrade the Manager to 4.3.

5.10. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

- Log in to the Manager machine.
- Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms \
```

All other repositories remain the same across Red Hat Virtualization releases.

- Update the setup packages:

```
# yum update ovirt\*setup\*
```

- Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```


5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
--disable=rhel-7-server-rhv-4.2-manager-rpms \
--disable=jb-eap-7-for-rhel-7-server-rpms \
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now change the cluster compatibility version to 4.3.

5.11. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

5.12. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute → Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



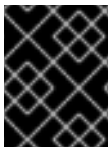
NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now change the data center compatibility version to 4.3.

5.13. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute → Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

5.14. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.
- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates](#).

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\); \1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

5. Restart the **httpd** service:

```
# systemctl restart httpd
```

6. Connect to the Administration Portal to confirm that the warning no longer appears.
7. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **`http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **`default_md = sha256:`**

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **`default_md = sha1`**, back up the existing configuration and change the default to **`sha256:`**

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **`ca.pem.new`**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$("
```

```

openssl \
  x509 \
  -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
  -noout \
  -subject \
  | sed \
  's;subject= \(.*\); \1;' \
  )"
/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
  --name="${name}" \
  --password=mypass \
  --subject="${subject}" \
  --keep-key
done

```

7. Restart the following services:

```

# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio-proxy

```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute → Hosts**.
 - b. Select the host and click **Management → Maintenance**.
 - c. Once the host is in maintenance mode, click **Installation → Enroll Certificate**.
 - d. Click **Management → Activate**.

CHAPTER 6. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.1 TO RED HAT VIRTUALIZATION 4.3

Upgrading your environment from 4.1 to 4.3 involves the following steps:

1. [Upgrade the database from PostgreSQL 9.2 to 9.5](#)
2. [Update the 4.1 Manager to the latest version of 4.1](#)
3. [Upgrade the Manager from 4.1 to 4.2](#)
4. [Upgrade the database from PostgreSQL 9.5 to 10.0](#)
5. [Upgrade the Manager from 4.2 to 4.3](#)
6. [Update the hosts](#)
7. [Update the compatibility version of the clusters](#)
8. [Reboot any running or suspended virtual machines to update their configuration](#)
9. [Update the compatibility version of the data centers](#)
10. [Replace SHA-1 certificates with SHA-256 certificates](#)
11. If you installed the technology preview version of Open Virtual Network (OVN) in 4.1, [update the OVN provider's networking plugin](#)

Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Subscribing to the Required Entitlements](#) for Red Hat Virtualization 4.1.

6.1. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.2 TO 9.5

Red Hat Virtualization 4.2 uses PostgreSQL 9.5 instead of PostgreSQL 9.2. If your databases are installed locally, the upgrade script will automatically upgrade them from version 9.2 to 9.5. However, if either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

1. Stop the service running on the machine:

- Stop the **ovirt-engine** service on the Manager machine:

```
# systemctl stop ovirt-engine
```

- Stop the **ovirt-engine-dwh** service on the Data Warehouse machine:

```
# systemctl stop ovirt-engine-dwhd
```

2. Enable the required repository to receive the PostgreSQL 9.5 package:
Enable either the Red Hat Virtualization Manager repository:

```
# subscription-manager repos --enable=rhel-7-server-rhv-4.2-manager-rpms
```

or the SCL repository:

```
# subscription-manager repos --enable rhel-server-rhscl-7-rpms
```

3. Install the PostgreSQL 9.5 packages:

```
# yum install rh-postgresql95 rh-postgresql95-postgresql-contrib
```

4. Stop and disable the PostgreSQL 9.2 service:

```
# systemctl stop postgresql
# systemctl disable postgresql
```

5. Upgrade the PostgreSQL 9.2 database to PostgreSQL 9.5:

```
# scl enable rh-postgresql95 -- postgresql-setup upgrade
```

6. Start and enable the **rh-postgresql95-postgresql.service** and check that it is running:

```
# systemctl start rh-postgresql95-postgresql.service
# systemctl enable rh-postgresql95-postgresql.service
# systemctl status rh-postgresql95-postgresql.service
```

Ensure that you see an output similar to the following:

```
rh-postgresql95-postgresql.service - PostgreSQL database server
Loaded: loaded (/usr/lib/systemd/system/rh-postgresql95-postgresql.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2018-05-07 08:48:27 CEST; 1h 59min ago
```

7. Log in to the database and enable the **uuid-osp** extension:

```
# su - postgres -c "scl enable rh-postgresql95 -- psql -d database-name"
```

8. Execute the following SQL commands:

```
# database-name=# DROP FUNCTION IF EXISTS uuid_generate_v1();
# database-name=# CREATE EXTENSION "uuid-osp";
```

- Copy the **pg_hba.conf** client configuration file from the 9.2 environment to your 9.5 environment:

```
# cp -p /var/lib/pgsql/data/pg_hba.conf /var/opt/rh/rh-postgresql95/lib/pgsql/data/pg_hba.conf
```

- Update the following parameters in **/var/opt/rh/rh-postgresql95/lib/pgsql/data/postgresql.conf**:

```
listen_addresses='*'
autovacuum_vacuum_scale_factor = 0.01
autovacuum_analyze_scale_factor = 0.075
autovacuum_max_workers = 6
maintenance_work_mem = 65536
max_connections = 150
work_mem = 8192
```

- Restart the PostgreSQL 9.5 service to apply the configuration changes:

```
# systemctl restart rh-postgresql95-postgresql.service
```

- Start the **ovirt-engine-dwhd** service:

```
# systemctl start ovirt-engine-dwhd
```

You can now update the Manager to the latest version of 4.1.

6.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

- Log in to the Manager machine.
- Check if updated packages are available:

```
# engine-upgrade-check
```

- Update the setup packages:

```
# yum update ovirt\*setup\*
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

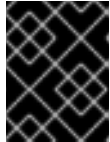
```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```


**NOTE**

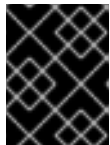
The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

5. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.2.

6.3. UPGRADING THE MANAGER FROM 4.1 TO 4.2

Upgrade the Red Hat Virtualization Manager from 4.1 to 4.2.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.2 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.2-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=jb-eap-7-for-rhel-7-server-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt-*setup*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

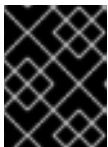
```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.1 repositories to ensure the system does not use any 4.1 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.1-rpms \
  --disable=rhel-7-server-rhv-4.1-manager-rpms \
  --disable=rhel-7-server-rhv-4-tools-rpms \
  --disable=jb-eap-7.0-for-rhel-7-server-rpms \
  --disable=jb-eap-7.1-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

6.4. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10

Red Hat Virtualization 4.3 uses PostgreSQL 10 instead of PostgreSQL 9.5. If your databases are installed locally, the upgrade script automatically upgrades them from version 9.5 to 10. However, if either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

1. Stop the service running on the machine:

- Stop the **ovirt-engine** service on the Manager machine:

```
# systemctl stop ovirt-engine
```

- Stop the **ovirt-engine-dwh** service on the Data Warehouse machine:

```
# systemctl stop ovirt-engine-dwhd
```

2. Enable the required repository to receive the PostgreSQL 10 package:
Enable either the Red Hat Virtualization Manager repository:

```
# subscription-manager repos --enable=rhel-7-server-rhv-4.3-manager-rpms
```

or the SCL repository:

```
# subscription-manager repos --enable rhel-server-rhscl-7-rpms
```

3. Install the PostgreSQL 10 packages:

```
# yum install rh-postgresql10 rh-postgresql10-postgresql-contrib
```

4. Stop and disable the PostgreSQL 9.5 service:

```
# systemctl stop rh-postgresql95-postgresql
# systemctl disable rh-postgresql95-postgresql
```

5. Upgrade the PostgreSQL 9.5 database to PostgreSQL 10:

```
# scl enable rh-postgresql10 -- postgresql-setup --upgrade-from=rh-postgresql95-postgresql
--upgrade
```

6. Start and enable the **rh-postgresql10-postgresql.service** and check that it is running:

```
# systemctl start rh-postgresql10-postgresql.service
# systemctl enable rh-postgresql10-postgresql.service
# systemctl status rh-postgresql10-postgresql.service
```

Ensure that you see output similar to the following:

```
rh-postgresql10-postgresql.service - PostgreSQL database server
Loaded: loaded (/usr/lib/systemd/system/rh-postgresql10-postgresql.service;
enabled; vendor preset: disabled)
Active: active (running) since ...
```

7. Copy the **pg_hba.conf** client configuration file from the PostgreSQL 9.5 environment to the PostgreSQL 10 environment:

```
# cp -p /var/opt/rh/rh-postgresql95/lib/pgsql/data/pg_hba.conf /var/opt/rh/rh-
postgresql10/lib/pgsql/data/pg_hba.conf
```

8. Update the following parameters in **/var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf**:

```
listen_addresses='*'
autovacuum_vacuum_scale_factor=0.01
autovacuum_analyze_scale_factor=0.075
autovacuum_max_workers=6
maintenance_work_mem=65536
max_connections=150
work_mem = 8192
```

9. Restart the PostgreSQL 10 service to apply the configuration changes:

```
# systemctl restart rh-postgresql10-postgresql.service
```

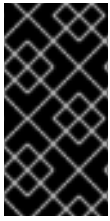
10. Start the **ovirt-engine-dwhd** service:

```
# systemctl start ovirt-engine-dwhd
```

You can now upgrade the Manager to 4.3.

6.5. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \  
--enable=rhel-7-server-rhv-4.3-manager-rpms \  
--enable=jb-eap-7.2-for-rhel-7-server-rpms \  

```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

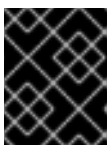
5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \  
--disable=rhel-7-server-rhv-4.2-manager-rpms \  
--disable=jb-eap-7-for-rhel-7-server-rpms \  

```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now update the hosts.

6.6. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md> for more information about the Ansible role used to automate the updates.

Red Hat recommends updating one cluster at a time.


Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.

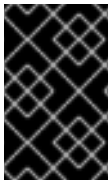
- **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
 6. Review the summary of the hosts and virtual machines that will be affected.
 7. Click **Upgrade**.

You can track the progress of host updates in the **Compute → Hosts** view, and in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

6.7. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute → Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

6.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

6.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.

2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

6.10. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.
- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates](#).

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
done
```



```

/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
  --name="{name}" \
  --password=mypass \
  --subject="{subject}" \
  --keep-key
done

```

- Restart the **httpd** service:

```
# systemctl restart httpd
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **http://*your-manager-fqdn*/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

- Log in to the Manager machine as the root user.
- Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```

# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf

```

- Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```

# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S)"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256

```

- Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

- Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

■

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
    )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

7. Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio-proxy
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute → Hosts**.
 - b. Select the host and click **Management → Maintenance**.
 - c. Once the host is in maintenance mode, click **Installation → Enroll Certificate**.
 - d. Click **Management → Activate**.

6.11. UPDATING OVN PROVIDERS INSTALLED IN RED HAT VIRTUALIZATION 4.1

If you installed an Open Virtual Network (OVN) provider in Red Hat Virtualization 4.1, you must manually edit its configuration for Red Hat Virtualization 4.2.

Procedure

1. Click **Administration** → **Providers** and select the OVN provider.
2. Click **Edit**.
3. Click the **Networking Plugin** text field and select **oVirt Network Provider for OVN** from the drop-down list.
4. Click **OK**.

CHAPTER 7. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.2 TO RED HAT VIRTUALIZATION 4.3

Upgrading your environment from 4.2 to 4.3 involves the following steps:

1. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade](#)
2. [Upgrade the database from PostgreSQL 9.5 to 10.0](#)
3. [Update the 4.2 Manager to the latest version of 4.2](#)
4. [Upgrade the Manager from 4.2 to 4.3](#)
5. [Update the hosts](#)
6. [Update the compatibility version of the clusters](#)
7. [Reboot any running or suspended virtual machines to update their configuration](#)
8. [Update the compatibility version of the data centers](#)
9. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

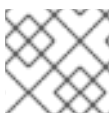
Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2.

7.1. ANALYZING THE ENVIRONMENT

Red Hat recommends running the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyses your environment and displays any known issues that may prevent you from performing an update and suggests how to resolve the issue.

The tool gathers detailed information about your system and presents it as an HTML file.



NOTE

The Log Collection Analysis tool is available from Red Hat Virtualization 4.2.5.

Procedure

1. Install the Log Collection Analysis tool on the Manager:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

7.2. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10

Red Hat Virtualization 4.3 uses PostgreSQL 10 instead of PostgreSQL 9.5. If your databases are installed locally, the upgrade script automatically upgrades them from version 9.5 to 10. However, if either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

1. Stop the service running on the machine:

- Stop the **ovirt-engine** service on the Manager machine:

```
# systemctl stop ovirt-engine
```

- Stop the **ovirt-engine-dwh** service on the Data Warehouse machine:

```
# systemctl stop ovirt-engine-dwhd
```

2. Enable the required repository to receive the PostgreSQL 10 package:
Enable either the Red Hat Virtualization Manager repository:

```
# subscription-manager repos --enable=rhel-7-server-rhv-4.3-manager-rpms
```

or the SCL repository:

```
# subscription-manager repos --enable rhel-server-rhscl-7-rpms
```

3. Install the PostgreSQL 10 packages:

```
# yum install rh-postgresql10 rh-postgresql10-postgresql-contrib
```

4. Stop and disable the PostgreSQL 9.5 service:

```
# systemctl stop rh-postgresql95-postgresql
# systemctl disable rh-postgresql95-postgresql
```

5. Upgrade the PostgreSQL 9.5 database to PostgreSQL 10:

```
# scl enable rh-postgresql10 -- postgresql-setup --upgrade-from=rh-postgresql95-postgresql
--upgrade
```

6. Start and enable the **rh-postgresql10-postgresql.service** and check that it is running:

```
# systemctl start rh-postgresql10-postgresql.service
# systemctl enable rh-postgresql10-postgresql.service
# systemctl status rh-postgresql10-postgresql.service
```

Ensure that you see output similar to the following:

```
rh-postgresql10-postgresql.service - PostgreSQL database server
Loaded: loaded (/usr/lib/systemd/system/rh-postgresql10-postgresql.service;
enabled; vendor preset: disabled)
Active: active (running) since ...
```

7. Copy the **pg_hba.conf** client configuration file from the PostgreSQL 9.5 environment to the PostgreSQL 10 environment:

```
# cp -p /var/opt/rh/rh-postgresql95/lib/pgsql/data/pg_hba.conf /var/opt/rh/rh-
postgresql10/lib/pgsql/data/pg_hba.conf
```

8. Update the following parameters in **/var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf**:

```
listen_addresses='*'
autovacuum_vacuum_scale_factor=0.01
autovacuum_analyze_scale_factor=0.075
autovacuum_max_workers=6
maintenance_work_mem=65536
max_connections=150
work_mem = 8192
```

9. Restart the PostgreSQL 10 service to apply the configuration changes:

```
# systemctl restart rh-postgresql10-postgresql.service
```

10. Start the **ovirt-engine-dwhd** service:

```
# systemctl start ovirt-engine-dwhd
```

You can now update the Manager to the latest version of 4.2.

7.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

- Update the setup packages:

```
# yum update ovirt\*setup\*
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.3.

7.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms \
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt*setup*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

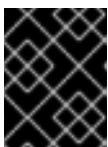
```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms \
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now update the hosts.

7.5. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful

during upgrades to new versions of Red Hat Virtualization. See <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md> for more information about the Ansible role used to automate the updates.

Red Hat recommends updating one cluster at a time.

Limitations


- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot

start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.

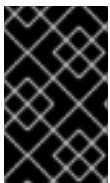
5. Click **Next**.
6. Review the summary of the hosts and virtual machines that will be affected.
7. Click **Upgrade**.

You can track the progress of host updates in the **Compute → Hosts** view, and in the **Events** section of the **Notification Drawer** () .

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

7.6. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure

1. In the Administration Portal, click **Compute → Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.




IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

7.7. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all

running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

7.8. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

7.9. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.
- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates](#).

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\); \1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

5. Restart the **httpd** service:

```
# systemctl restart httpd
```

6. Connect to the Administration Portal to confirm that the warning no longer appears.
7. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **`http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **`default_md = sha256`**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **`default_md = sha1`**, back up the existing configuration and change the default to **`sha256`**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **`ca.pem.new`**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$("
```

```

openssl \
  x509 \
  -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
  -noout \
  -subject \
  | sed \
  's;subject= \(.*\); \1;' \
  )"
/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
  --name="${name}" \
  --password=mypass \
  --subject="${subject}" \
  --keep-key
done

```

7. Restart the following services:

```

# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio-proxy

```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute → Hosts**.
 - b. Select the host and click **Management → Maintenance**.
 - c. Once the host is in maintenance mode, click **Installation → Enroll Certificate**.
 - d. Click **Management → Activate**.

PART III. UPGRADING A SELF-HOSTED ENGINE ENVIRONMENT

CHAPTER 8. UPGRADING A SELF-HOSTED ENGINE FROM 4.0 TO RED HAT VIRTUALIZATION 4.3

The 4.0 compatibility version is not supported after Red Hat Virtualization 4.2. Therefore, when upgrading from Red Hat Virtualization 4.0 you must update the cluster and data center compatibility versions to at least 4.1 before upgrading the Manager from 4.2 to 4.3, then update the compatibility versions again after completing the Manager upgrades.

You must also update the hosts before updating the compatibility versions, but only need to do so once. The host repositories stay the same across Red Hat Virtualization versions, so the hosts will already be upgraded to the latest version after a single update.

Upgrading your environment from 4.0 to 4.3 involves the following steps:

1. [Place the environment in global maintenance mode](#)
2. [Update the 4.0 Manager to the latest version of 4.0](#)
3. [Upgrade the Manager from 4.0 to 4.1](#)
4. [Upgrade the Manager from 4.1 to 4.2](#)
5. [Disable global maintenance mode](#)
6. [Update the hosts](#)
7. [Update the compatibility version of the clusters to 4.2](#)
8. [Reboot any running or suspended virtual machines to update their configuration to 4.2](#)
9. [Update the compatibility version of the data centers to 4.2](#)
10. [Place the environment in global maintenance mode](#)
11. [Upgrade the Manager from 4.2 to 4.3](#)
12. [Disable global maintenance mode](#)
13. [Update the compatibility version of the clusters](#)
14. [Reboot any running or suspended virtual machines to update their configuration to the latest version](#)
15. [Update the compatibility version of the data centers](#)
16. [Replace SHA-1 certificates with SHA-256 certificates](#)

Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).

- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Subscribing to the Required Entitlements](#) for Red Hat Virtualization 4.0.

8.1. ENABLING GLOBAL MAINTENANCE MODE

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in maintenance mode.

8.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager virtual machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

**NOTE**

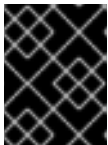
The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

5. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

8.3. UPGRADING THE MANAGER FROM 4.0 TO 4.1

Upgrade the Red Hat Virtualization Manager from 4.0 to 4.1.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager virtual machine.
2. Enable the Red Hat Virtualization 4.1 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.1-rpms \
  --enable=rhel-7-server-rhv-4-tools-rpms \
  --enable=jb-eap-7.1-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.0 repositories to ensure the system does not use any 4.0 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.0-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms \
  --disable=jb-eap-7.0-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```

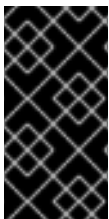


IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

8.4. UPGRADING THE MANAGER FROM 4.1 TO 4.2

Upgrade the Red Hat Virtualization Manager from 4.1 to 4.2.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager virtual machine.
2. Enable the Red Hat Virtualization 4.2 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.2-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=jb-eap-7-for-rhel-7-server-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

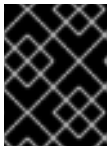
```
# engine-setup
```

- 5. Disable the Red Hat Virtualization 4.1 repositories to ensure the system does not use any 4.1 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.1-rpms \
  --disable=rhel-7-server-rhv-4.1-manager-rpms \
  --disable=rhel-7-server-rhv-4-tools-rpms \
  --disable=jb-eap-7.0-for-rhel-7-server-rpms \
  --disable=jb-eap-7.1-for-rhel-7-server-rpms
```

- 6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

8.5. DISABLING GLOBAL MAINTENANCE MODE

Procedure

1. Log in to the Manager virtual machine.
2. Shut down the virtual machine.
3. Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

4. Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```



NOTE

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

You must now update the hosts before you can update the cluster and data center compatibility versions. Update the self-hosted engine nodes first, and then any standard hosts. The procedure is the same for both host types.

8.6. UPDATING INDIVIDUAL HOSTS

Use the host upgrade manager to update individual hosts directly from the Administration Portal.



NOTE

The upgrade manager only checks hosts with a status of **Up** or **Non-operational**, but not **Maintenance**.


Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure

1. Ensure that the correct repositories are enabled. To view a list of currently enabled repositories, run **yum repolist**.
 - For Red Hat Virtualization Hosts:


```
# subscription-manager repos --enable=rhel-7-server-rhvh-4-rpms
```
 - For Red Hat Enterprise Linux hosts:


```
# subscription-manager repos \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```
2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Installation** → **Check for Upgrade** and click **OK**.
Open the **Notification Drawer** () and expand the **Events** section to see the result.

4. If an update is available, click **Installation** → **Upgrade**.
5. Click **OK** to update the host. Running virtual machines are migrated according to their migration policy. If migration is disabled for any virtual machines, you are prompted to shut them down. The details of the host are updated in **Compute** → **Hosts** and the status transitions through these stages:
 - **Maintenance**
 - **Installing**
 - **Reboot**
 - **Up**If any virtual machines were migrated off the host, they are now migrated back.



NOTE

If the update fails, the host's status changes to **Install Failed**. From **Install Failed** you can click **Installation** → **Upgrade** again.

Repeat this procedure for each host in the Red Hat Virtualization environment.

You can now change the cluster compatibility version to 4.2.

8.7. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

8.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute → Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now change the data center compatibility version to 4.2.

8.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

8.10. ENABLING GLOBAL MAINTENANCE MODE

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in maintenance mode.

8.11. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager virtual machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \  
  --enable=rhel-7-server-rhv-4.3-manager-rpms \  
  --enable=jb-eap-7.2-for-rhel-7-server-rpms \  
  --enable=rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:


```
# yum update ovirt*setup*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

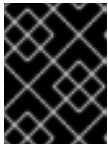
```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms \
```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

8.12. DISABLING GLOBAL MAINTENANCE MODE

Procedure

1. Log in to the Manager virtual machine.
2. Shut down the virtual machine.
3. Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

4. Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```

**NOTE**

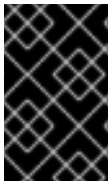
When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

8.13. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

**IMPORTANT**

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.


Procedure

1. In the Administration Portal, click **Compute → Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

**IMPORTANT**

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

8.14. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes

made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

8.15. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

8.16. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat

Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates.](#)

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

5. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name}".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;'\
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

6. Restart the **httpd** service:

```
# systemctl restart httpd
```

7. Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

7. On the Manager, re-sign the certificates:

```

for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
    )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done

```

8. Restart the following services:

```

# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio-proxy

```

9. Log in to one of the self-hosted engine nodes and disable global maintenance:

```

# hosted-engine --set-maintenance --mode=none

```

10. Connect to the Administration Portal to confirm that the warning no longer appears.
11. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
12. Enroll the certificates on the hosts. Repeat the following procedure for each host.
- In the Administration Portal, click **Compute** → **Hosts**.
 - Select the host and click **Management** → **Maintenance**.
 - Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - Click **Management** → **Activate**.

CHAPTER 9. UPGRADING A SELF-HOSTED ENGINE FROM 4.1 TO RED HAT VIRTUALIZATION 4.3

Upgrading a self-hosted engine environment from version 4.1 to 4.2 involves the following steps:

1. [Place the environment in global maintenance mode](#)
2. [Update the 4.1 Manager to the latest version of 4.1](#)
3. [Upgrade the Manager from 4.1 to 4.2](#)
4. [Upgrade the Manager from 4.2 to 4.3](#)
5. [Disable global maintenance mode](#)
6. [Update the self-hosted engine nodes, and any standard hosts](#)
7. [Update the compatibility version of the clusters](#)
8. [Reboot any running or suspended virtual machines to update their configuration](#)
9. [Update the compatibility version of the data centers](#)
10. If you installed the technology preview version of Open Virtual Network (OVN) in 4.1, [update the OVN provider's networking plugin](#)
11. [Replace SHA-1 certificates with SHA-256 certificates](#)

Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Subscribing to the Required Entitlements](#) for Red Hat Virtualization 4.1.

9.1. ENABLING GLOBAL MAINTENANCE MODE

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in maintenance mode.

9.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager virtual machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

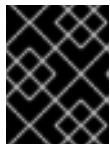


IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

5. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```


**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

9.3. UPGRADING THE MANAGER FROM 4.1 TO 4.2

Upgrade the Red Hat Virtualization Manager from 4.1 to 4.2.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager virtual machine.
2. Enable the Red Hat Virtualization 4.2 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.2-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=jb-eap-7-for-rhel-7-server-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt-*setup*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

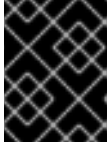
```
# engine-setup
```

5. Disable the Red Hat Virtualization 4.1 repositories to ensure the system does not use any 4.1 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.1-rpms \
  --disable=rhel-7-server-rhv-4.1-manager-rpms \
  --disable=rhel-7-server-rhv-4-tools-rpms \
  --disable=jb-eap-7.0-for-rhel-7-server-rpms \
  --disable=jb-eap-7.1-for-rhel-7-server-rpms
```

6. Update the base operating system:

```
# yum update
```

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the upgrade.

9.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager virtual machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms \
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

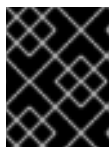
```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms \
```

6. Update the base operating system:

```
# yum update
```

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the upgrade.

9.5. DISABLING GLOBAL MAINTENANCE MODE

Procedure

1. Log in to the Manager virtual machine.
2. Shut down the virtual machine.
3. Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

4. Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```

**NOTE**

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

9.6. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md> for more information about the Ansible role used to automate the updates.

Red Hat recommends updating one cluster at a time.


Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
6. Review the summary of the hosts and virtual machines that will be affected.

7. Click **Upgrade**.

You can track the progress of host updates in the **Compute → Hosts** view, and in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

9.7. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

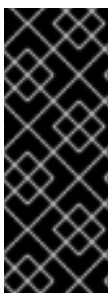


IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute → Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

9.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes

made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

9.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

9.10. UPDATING OVN PROVIDERS INSTALLED IN RED HAT VIRTUALIZATION 4.1

If you installed an Open Virtual Network (OVN) provider in Red Hat Virtualization 4.1, you must manually edit its configuration for Red Hat Virtualization 4.2.

Procedure

1. Click **Administration** → **Providers** and select the OVN provider.

2. Click **Edit**.
3. Click the **Networking Plugin** text field and select **oVirt Network Provider for OVN** from the drop-down list.
4. Click **OK**.

9.11. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.
- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates](#).

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

5. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
```

```

        -subject \
    | sed \
        's;subject= \(.*\);1;' \
    )"
/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done

```

- Restart the **httpd** service:

```
# systemctl restart httpd
```

- Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

- Log in to the Manager machine as the root user.
- Check whether **`/etc/pki/ovirt-engine/openssl.conf`** includes the line **`default_md = sha256`**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **`default_md = sha1`**, back up the existing configuration and change the default to **`sha256`**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

- Re-sign the CA certificate by backing it up and creating a new certificate in **`ca.pem.new`**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S)"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

- Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```


- Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

- Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

- On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
    )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

- Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio-proxy
```

- Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

12. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute** → **Hosts**.
 - b. Select the host and click **Management** → **Maintenance**.
 - c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - d. Click **Management** → **Activate**.

CHAPTER 10. UPGRADING A SELF-HOSTED ENGINE FROM 4.2 TO RED HAT VIRTUALIZATION 4.3

Upgrading a self-hosted engine environment from version 4.2 to 4.3 involves the following steps:

1. Use the [Log Collection Analysis tool](#) to check for issues that might prevent a successful upgrade
2. Place the environment in global maintenance mode
3. Update the 4.2 Manager to the latest version of 4.2
4. Upgrade the Manager from 4.2 to 4.3
5. Disable global maintenance mode
6. Upgrade the self-hosted engine nodes, and any standard hosts
7. Update the compatibility version of the clusters
8. Reboot any running or suspended virtual machines to update their configuration
9. Update the compatibility version of the data centers
10. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.3. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- Ensure the hosts have the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Host Repository](#) for RHVH, or [Enabling the Red Hat Enterprise Linux Host Repositories](#) for RHEL hosts.
- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2.

10.1. ANALYZING THE ENVIRONMENT

Red Hat recommends running the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyses your environment and displays any known issues that may prevent you from performing an update and suggests how to resolve the issue.

The tool gathers detailed information about your system and presents it as an HTML file.



NOTE

The Log Collection Analysis tool is available from Red Hat Virtualization 4.2.5.

Procedure

1. Install the Log Collection Analysis tool on the Manager:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

10.2. ENABLING GLOBAL MAINTENANCE MODE

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in maintenance mode.

10.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager virtual machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup**

script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

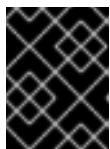
When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

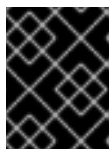


IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

5. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

10.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager virtual machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \  
--enable=rhel-7-server-rhv-4.3-manager-rpms \  
--enable=jb-eap-7.2-for-rhel-7-server-rpms \  

```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \  
--disable=rhel-7-server-rhv-4.2-manager-rpms \  
--disable=jb-eap-7-for-rhel-7-server-rpms \  

```

6. Update the base operating system:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

10.5. DISABLING GLOBAL MAINTENANCE MODE

Procedure

1. Log in to the Manager virtual machine.
2. Shut down the virtual machine.
3. Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

4. Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```



NOTE

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

10.6. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md> for more information about the Ansible role used to automate the updates.

Red Hat recommends updating one cluster at a time.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.


4. Configure the options:

- **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
- **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
- **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
- **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
- **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.

5. Click **Next**.

6. Review the summary of the hosts and virtual machines that will be affected.

7. Click **Upgrade**.

You can track the progress of host updates in the **Compute → Hosts** view, and in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

10.7. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

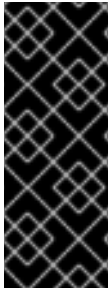


IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

10.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_configuration_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Reboot**.

When the virtual machine starts, the new compatibility version is automatically applied.

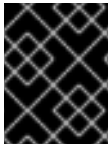


NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

10.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

10.10. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.3 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for systems upgraded from 4.1 or earlier, one of the following is required:

- [Prevent warning messages from appearing in your browser when connecting to the Administration Portal](#). These warnings may either appear as pop-up windows or in the browser's **Web Console** window. This option is not required if you already replaced the Red Hat Virtualization Manager's Apache SSL certificate after the upgrade. However, if the certificate was signed with SHA-1, you should replace it with an SHA-256 certificate. For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.
- [Replace the SHA-1 certificates throughout the system with SHA-256 certificates](#).

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

5. On the Manager, re-sign the Apache certificate:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

6. Restart the **httpd** service:

```
# systemctl restart httpd
```

7. Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether **/etc/pki/ovirt-engine/openssl.conf** includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager SSL Certificate](#) in the *Administration Guide*.

6. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

7. On the Manager, re-sign the certificates:

```
for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
    )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key
done
```

8. Restart the following services:

```
# systemctl restart httpd
```

```
# systemctl restart ovirt-engine  
# systemctl restart ovirt-websocket-proxy  
# systemctl restart ovirt-imageio-proxy
```

9. Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

10. Connect to the Administration Portal to confirm that the warning no longer appears.
11. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **`http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
12. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute** → **Hosts**.
 - b. Select the host and click **Management** → **Maintenance**.
 - c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - d. Click **Management** → **Activate**.

PART IV. APPENDICES

APPENDIX A. UPDATES BETWEEN MINOR RELEASES

To update from your current version of 4.3 to the latest version of 4.3, update the Manager and then update the hosts.

A.1. ANALYZING THE ENVIRONMENT

Red Hat recommends running the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyses your environment and displays any known issues that may prevent you from performing an update and suggests how to resolve the issue.

The tool gathers detailed information about your system and presents it as an HTML file.



NOTE

The Log Collection Analysis tool is available from Red Hat Virtualization 4.2.5.

Procedure

1. Install the Log Collection Analysis tool on the Manager:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

To update a standalone Manager, follow the standard procedure for minor updates:

A.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager machine.
2. Check if updated packages are available:

```
# engine-upgrade-check
```

3. Update the setup packages:

```
# yum update ovirt\*setup\*
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

A.3. UPDATING A SELF-HOSTED ENGINE

To update a self-hosted engine from your current version of 4.3 to the latest version of 4.3, you must place the environment in global maintenance mode and then follow the standard procedure for updating between minor versions.

Enabling Global Maintenance Mode

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

- Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```


2. Confirm that the environment is in maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in maintenance mode.

Updating the Red Hat Virtualization Manager

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Log in to the Manager virtual machine.
2. Log in to the Manager machine.
3. Check if updated packages are available:

```
# engine-upgrade-check
```

4. Update the setup packages:

```
# yum update ovirt\*setup\*
```

5. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

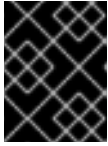


IMPORTANT

The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

6. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

Disabling Global Maintenance Mode

Procedure

1. Log in to the Manager virtual machine.
2. Shut down the virtual machine.
3. Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

4. Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```



NOTE

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

A.4. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md> for more information about the Ansible role used to automate the updates.

Red Hat recommends updating one cluster at a time.


Limitations

- On RHVH, the update only preserves modified content in the `/etc` and `/var` directories. Modified data in other paths is overwritten during an update.

- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
6. Review the summary of the hosts and virtual machines that will be affected.
7. Click **Upgrade**.

You can track the progress of host updates in the **Compute → Hosts** view, and in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

You can also update hosts individually:

A.5. UPDATING INDIVIDUAL HOSTS

Use the host upgrade manager to update individual hosts directly from the Administration Portal.



NOTE

The upgrade manager only checks hosts with a status of **Up** or **Non-operational**, but not **Maintenance**.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure


1. Ensure that the correct repositories are enabled. To view a list of currently enabled repositories, run **yum repolist**.

- For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhel-7-server-rhvh-4-rpms
```

- For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```

2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Installation** → **Check for Upgrade** and click **OK**.
Open the **Notification Drawer** () and expand the **Events** section to see the result.
4. If an update is available, click **Installation** → **Upgrade**.
5. Click **OK** to update the host. Running virtual machines are migrated according to their migration policy. If migration is disabled for any virtual machines, you are prompted to shut them down. The details of the host are updated in **Compute** → **Hosts** and the status transitions through these stages:
 - **Maintenance**
 - **Installing**
 - **Reboot**
 - **Up**
If any virtual machines were migrated off the host, they are now migrated back.

**NOTE**

If the update fails, the host's status changes to **Install Failed**. From **Install Failed** you can click **Installation** → **Upgrade** again.

Repeat this procedure for each host in the Red Hat Virtualization environment.

Red Hat recommends updating the hosts from the Administration Portal. However, you can update the hosts using **yum update** instead:

A.6. MANUALLY UPDATING HOSTS

You can use the **yum** command to update your hosts. Update your systems regularly, to ensure timely application of security and bug fixes.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If migration is enabled at the cluster level, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.

- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure

1. Ensure the correct repositories are enabled. You can check which repositories are currently enabled by running **yum repolist**.

- For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhel-7-server-rhvh-4-rpms
```

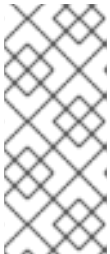
- For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
  --enable=rhel-7-server-ansible-2-rpms
```

2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Management** → **Maintenance**.
4. Update the host:

```
# yum update
```

5. Reboot the host to ensure all updates are correctly applied.



NOTE

Check the `imgbased` logs to see if any additional package updates have failed for a Red Hat Virtualization Host. If some packages were not successfully reinstalled after the update, check that the packages are listed in `/var/imgbased/persisted-rpms`. Add any missing packages then run **rpm -Uvh /var/imgbased/persisted-rpms/***.

Repeat this process for each host in the Red Hat Virtualization environment.

APPENDIX B. UPDATING THE LOCAL REPOSITORY FOR AN OFFLINE RED HAT VIRTUALIZATION MANAGER INSTALLATION

If your Red Hat Virtualization Manager is hosted on a system that receives packages via FTP from a local repository, you must regularly synchronize the repository to download package updates from the Content Delivery Network, then update or upgrade your Manager system. Updated packages address security issues, fix bugs, and add enhancements.

1. On the system hosting the repository, synchronize the repository to download the most recent version of each available package:

```
# reposync -l --newest-only /var/ftp/pub/rhevrepo
```

This command might download a large number of packages, and take a long time to complete.

2. Ensure that the repository is available on the Manager system, and then update or upgrade the Manager system. See [Updating the Red Hat Virtualization Manager](#) for information on updating the Manager between minor versions. See [Red Hat Virtualization Upgrade Overview](#) for information on upgrading between major versions.

APPENDIX C. UPGRADING TO RED HAT VIRTUALIZATION MANAGER 4.3 WITH `ovirt-fast-forward-upgrade`

If you have Red Hat Virtualization 4.0 or later installed, you can upgrade the Manager to the latest version with the `ovirt-fast-forward-upgrade` tool. `ovirt-fast-forward-upgrade` detects the current version of the Manager and checks for available upgrades. If an upgrade is available, the tool upgrades the Manager to the next major version, and continues to upgrade the Manager until the latest version is installed.



NOTE

`ovirt-fast-forward-upgrade` upgrades the Manager. See [Section A.4, “Updating All Hosts in a Cluster”](#) to upgrade the hosts.

Upgrading with `ovirt-fast-forward-upgrade`

1. Install the `ovirt-fast-forward-upgrade` tool:

```
# yum install ovirt-fast-forward-upgrade
```

2. Run the following command to upgrade the Manager, while creating a backup of the current version:

```
# ovirt-fast-forward-upgrade --backup --backup-dir=/backup
```



NOTE

Red Hat recommends using the `--backup` and `--backup-dir` options to create a backup of the current Manager. If a backup directory is not specified, the backup is saved in `/tmp`.

The `--backup` option is a wrapper for the `engine-backup` tool and is equivalent to running the following command:

```
# engine-backup --scope=all --mode=backup --file=file_name --log=log_file_name
```

To restore your backup, run `engine-backup` in `restore` mode:

```
# engine-backup --mode=restore
```

See [Backing Up and Restoring the Red Hat Virtualization Manager](#) in the *Administration Guide* for details.

Alternatively, to upgrade without creating a backup, run the following command:

```
# ovirt-fast-forward-upgrade
```

3. If there are errors, check the log: `/var/log/ovirt-engine/ovirt-fast-forward-upgrade.log`.

