Red Hat

Red Hat Virtualization 4.2

Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Last Updated: 2020-06-03

Red Hat Virtualization 4.2 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

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

This guide explains how to upgrade your current environment to Red Hat Virtualization 4.2.

Two upgrade paths are documented here:

- **Local Database**: Both Data Warehouse and the Manager database are installed on the Manager.
- **Remote Database**: Data Warehouse is on a separate machine.

To upgrade a self-hosted engine, see Upgrading a Self-Hosted Engine Environment in the *Self-Hosted Engine Guide*.

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
3.6	4.2	**Local database environment:** Chapter 2, *Upgrading from 3.6 to Red Hat Virtualization 4.2* **Remote database environment:** Chapter 5, *Upgrading a Remote Database Environment from 3.6 to Red Hat Virtualization 4.2*
4.0	4.2	**Local database environment:** Chapter 3, *Upgrading from 4.0 to Red Hat Virtualization 4.2* **Remote database environment:** Chapter 6, *Upgrading a Remote Database Environment from 4.0 to Red Hat Virtualization 4.2*
4.1	4.2	**Local database environment:** Chapter 4, *Upgrading from 4.1 to Red Hat Virtualization 4.2* **Remote database environment:** Chapter 7, *Upgrading a Remote Database Environment from 4.1 to Red Hat Virtualization 4.2*
4.2.x	4.2.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 3.6 TO RED HAT VIRTUALIZATION 4.2

You cannot upgrade the Manager directly from 3.6 to 4.2. You must upgrade your environment in the following sequence:

1. Update the 3.6 Manager to the latest version of 3.6
2. Upgrade the Manager from 3.6 to 4.0
3. Upgrade the Manager from 4.0 to 4.1
4. Upgrade the Manager from 4.1 to 4.2
5. Upgrade the hosts

   > **NOTE**
   >
   > If you are upgrading RHEV-H hosts that use local storage, see Appendix C, *Upgrading from RHEV-H 3.6 to RHVH 4.2 While Preserving Local Storage* .

6. Update the compatibility version of the clusters
7. Update the compatibility version of the data centers
8. If you backed up an ISO storage domain that was hosted on the 3.6 Manager, restore the ISO domain in the upgraded environment
9. Replace SHA-1 certificates with SHA-256 certificates

2.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

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

Procedure

1. On the Red Hat Virtualization Manager machine, check if updated packages are available:

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

2. Update the setup packages:

   ```
   # yum update rhevm-setup
   ```

3. Update the Red Hat Virtualization Manager. 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
   ```

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 may 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.

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

```
# yum update
```

IMPORTANT

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

2.2. UPGRADING THE MANAGER FROM 3.6 TO 4.0

In Red Hat Enterprise Virtualization 3.6, the Manager runs on Red Hat Enterprise Linux 6. An in-place upgrade of the Manager machine to Red Hat Enterprise Linux 7 is not supported. To upgrade from 3.6 to 4.0, you must install a new 4.0 Manager on Red Hat Enterprise Linux 7, and restore a backup of the 3.6 Manager database on the new Manager.

If any optional extension packages, such as **ovirt-engine-extension-aaa-ldap**, **ovirt-engine-extension-aaa-misc**, or **ovirt-engine-extension-logger-log4j** are installed on Red Hat Enterprise Virtualization Manager 3.6, they must be installed on the upgraded Manager before running **engine-setup**. The settings for these package extensions are not migrated as part of the upgrade. You can copy the configuration files to the same device or machine as the 3.6 Manager backup file.

NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 3.6 before attempting the procedure.

- Directory servers configured using the domain management tool are not supported after Red Hat Enterprise Virtualization 3.6. If your directory servers are configured using the domain management tool, migrate to the new extension-based provider before backing up the environment. See Migrating from the Legacy Provider to the New Extension-Based Provider in the *Red Hat Enterprise Virtualization 3.6 Administration Guide* for more information.

Procedure

Procedure

1. On the 3.6 Manager, back up the environment:

   ```
   # engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
   ```

2. Copy the backup file to a suitable device or machine.

3. If the ISO storage domain is hosted on the Manager machine, back up the contents of **/var/lib/exports/iso**:

   ```
   # cd /var/lib/exports/iso
   # tar zcf iso_domain.tar.gz UUID
   ```

   You will restore the ISO storage backup file after the upgrade.

4. Install Red Hat Enterprise Linux 7. See the *Red Hat Enterprise Linux Installation Guide* .
   If you are installing RHEL 7 on a new machine, you must configure it to have the same fully qualified domain name as the 3.6 Manager machine, and update your DNS so that the FQDN correlates to the IP address of the new machine.

5. Install the Red Hat Virtualization 4.0 packages:

   a. Register your system with the Content Delivery Network, entering your Customer Portal user name and password when prompted:

      ```
      # subscription-manager register
      ```

   b. Find the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscription pools and record the pool IDs:

      ```
      # subscription-manager list --available
      ```

   c. Use the pool IDs to attach the entitlements to the system:

      ```
      # subscription-manager attach --pool=pool_id
      ```

   d. Configure the repositories:

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

   e. Ensure all packages are up to date:

      ```
      # yum update
      ```

   f. Install the **rhevm** package and dependencies:

      ```
      # yum install rhevm
      ```

6. Copy the backup file to the 4.0 Manager machine and restore the backup:

```
# engine-backup --mode=restore --file=backup.bck --log=restore.log \
   --provision-db --provision-dwh-db --restore-permissions
```

NOTE

If the backup contained grants for extra database users, this command will create the extra users with random passwords. You must change these passwords manually if the extra users require access to the restored system. See https://access.redhat.com/articles/2686731.

NOTE

Use the **--provision-dwh-db** option if the backup contains Data Warehouse data.

Red Hat Enterprise Virtualization Reports has been deprecated in Red Hat Virtualization 4.0 and will not be restored. See BZ#1340810 for more information.

7. Install optional extension packages if they were installed on the 3.6 Manager machine:

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc ovirt-engine-
extension-logger-log4j
```

NOTE

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

8. Decommission the 3.6 Manager machine if you are using a different machine for the 4.0 Manager.

9. Run **engine-setup** to configure the Manager:

```
# engine-setup
```

NOTE

If you use external CA to sign HTTPS certificates, follow the steps in Replacing the Red Hat Virtualization Manager SSL Certificate in the *Administration Guide* to log in to the Administration Portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works.

2.3. 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 will attempt 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. 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.

2. Update the setup packages:

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

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

   ```
   # engine-setup
   ```

4. 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
   ```

5. Update the base operating system:

   ```
   # yum update
   ```

6. Reboot the machine.

2.4. 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 will attempt 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. 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-2.9-rpms
   ```

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

2. Update the setup packages:

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

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

   ```
   # engine-setup
   ```

   > **NOTE**
   >
   > If you changed the default trust keystore password, you might get a keystore certificate error. If so, update the configuration to reflect the correct password. For more information, see *RHV 4.2 - Failed to import provider certificate into the external provider keystore*

4. 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
   ```

5. Update the base operating system:

   ```
   # yum update
   ```

6. Reboot the machine.

You can now update the hosts.

2.5. UPDATING THE HOSTS

IMPORTANT

Use this procedure to update Red Hat Enterprise Linux hosts or Red Hat Virtualization Hosts (RHVH).

Legacy Red Hat Enterprise Virtualization Hypervisors (RHEV-H) are not supported in Red Hat Virtualization; you must reinstall them with RHVH. See Installing Red Hat Virtualization Host in the *Installation Guide*. If you need to preserve local storage on the host, see Appendix C, *Upgrading from RHEV-H 3.6 to RHVH 4.2 While Preserving Local Storage*.

If you are not sure whether you are using RHEV-H or RHVH, type **imgbase check**. If the command fails, the host is RHEV-H. If it succeeds, the host is RHVH.

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager.

NOTE

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

IMPORTANT

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

Prerequisites

- 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.
- Ensure that the cluster contains more than one host before performing an update. Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve for its hosts to perform maintenance. Otherwise, the virtual machine migration operation will hang and fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed must be shut down before updating the host.

Procedure

1. If your Red Hat Enterprise Linux hosts are locked to version 7.3, as described in https://access.redhat.com/solutions/3194482, set them to the general RHEL 7 version before updating (to view the version number, type **subscription-manager release --show**):

```
# subscription-manager release --set=7Server
```

2. Disable your current repositories:

```
# subscription-manager repos --disable='*'
```

3. Ensure that the correct repositories are enabled (to view a list of currently enabled repositories, type **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-2.9-rpms
     ```

4. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
5. Click **Installation** → **Check for Upgrade** and click **OK**.

   Click the **Events and alerts notification** icon (🔔) and expand the **Events** section to see the result.
6. If an update is available, click **Installation** → **Upgrade**.
7. Click **OK** to update the host. Running virtual machines will be migrated according to their migration policy. If migration is disabled for any virtual machines, you will be 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.

2.6. 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. See Section A.3, "Updating the Hosts" for more information on updating hosts.

Procedure

1. Click **Compute → Clusters** and select the cluster to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Cluster Compatibility Version** confirmation window.
5. Click **OK** to confirm.

IMPORTANT

An error message may 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.

After you update the cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by restarting them from within the Manager, or using the REST API, instead of within the guest operating system. Virtual machines will continue to run in the previous cluster compatibility level until they are restarted. Those virtual machines that require a restart are marked with the pending changes icon (⚠). You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview; you must first commit or undo the preview.

The self-hosted engine virtual machine does not need to be restarted.

Once you have updated the compatibility version of all clusters in a data center, you can then change the compatibility version of the data center itself.

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 that the data center is intended to be compatible with. 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 all the clusters in your data center to a level that supports your desired compatibility level.

Procedure

1. Click **Compute → Data Centers** and select the data center to change.

2. Click **Edit**.

3. Change the **Compatibility Version** to the desired value.

4. Click **OK** to open the **Change Data Center Compatibility Version** confirmation window.

5. Click **OK** to confirm.

2.8. MIGRATING THE ISO DOMAIN FROM 3.6

Migrate the ISO domain from 3.6 to the current version of Red Hat Virtualization, using the **iso_domain.tar.gz** backup file that you created during the upgrade from 3.6 to 4.0.

IMPORTANT

The new directory for the ISO domain must not be on the Manager machine.

NOTE

The ISO domain is deprecated in Red Hat Virtualization 4.2, and will be removed in a future version. Red Hat recommends uploading ISO images to a data storage domain. See Uploading Images to a Data Storage Domain in the *Administration Guide*.

1. Create an export directory on the storage server and set its permissions:

```
# mkdir -p /var/lib/exports/iso
# chown -R 36:36 /var/lib/exports/
```

2. Extract the ISO domain backup to this directory:

```
# cd /var/lib/exports/iso
# tar zxf iso_domain.tar.gz
```

3. Set the SELinux context for the files in the export directory:

```
# chcon -R system_u:object_r:public_content_rw_t:s0 /var/lib/exports/iso/
```

4. Create **/etc/exports.d/ovirt-engine-iso-domain.exports** with the following line:

```
/var/lib/exports/iso  *(rw)
```

5. Edit the following lines in **/etc/sysconfig/nfs**:

```
RPCMOUNTDOPTS="-p 892"
(..snip..)
STATDARGS="-p 662 -o 2020"
(..snip..)
LOCKD_UDPPORT=32769
LOCKD_TCPPORT=32803
RPCRQUOTAOPTS="-p 875"
```

6. Enable the **nfs** service:

```
# systemctl enable nfs
# systemctl start nfs
```

7. Allow services and ports with **firewalld**:

```
# firewall-cmd --add-service={nfs,rpc-bind}
# firewall-cmd --add-service={nfs,rpc-bind} --permanent
# firewall-cmd --add-port=
{32769/udp,32803/tcp,662/tcp,662/udp,875/tcp,875/udp,892/tcp,892/udp}
# firewall-cmd --add-port=
{32769/udp,32803/tcp,662/tcp,662/udp,875/tcp,875/udp,892/tcp,892/udp} --permanent
```

8. In the Administration Portal, update the ISO domain's storage path:

   a. Click **Storage → Domains**.

   b. Click the ISO domain's name to go to the details view.

   c. Click the **Data Center** tab and click **Maintenance**.

   d. When the ISO domain is in maintenance mode, click **Manage Domain**.

   e. Change the **Export Path** to point to the new directory, for example: *storage.example.com*:/var/lib/exports/iso

   f. Click **OK**.

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

Red Hat Virtualization 4.2 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed 4.2 systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for upgraded systems one of the following is recommended:

- 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 SSL 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 4.0 TO RED HAT VIRTUALIZATION 4.2

You cannot upgrade the Manager directly from 4.0 to 4.2. You must upgrade your environment in the following sequence:

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. Upgrade the hosts
5. Update the compatibility version of the clusters
6. Update the compatibility version of the data centers
7. Replace SHA-1 certificates with SHA-256 certificates

3.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

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

Procedure

1. On the Red Hat Virtualization Manager machine, check if updated packages are available:

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

2. Update the setup packages:

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

3. Update the Red Hat Virtualization Manager. 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
   ```

   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 may 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.

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

```
# yum update
```

> **IMPORTANT**
>
> If any kernel packages were updated, reboot the host to complete the update.

3.2. 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 will attempt 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. 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.

2. Update the setup packages:

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

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

```
# engine-setup
```

4. 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
```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

3.3. 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 will attempt 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. 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-2.9-rpms
   ```

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

2. Update the setup packages:

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

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

   ```
   # engine-setup
   ```

   #### NOTE

   If you changed the default trust keystore password, you might get a keystore certificate error. If so, update the configuration to reflect the correct password. For more information, see *RHV 4.2 - Failed to import provider certificate into the external provider keystore*

4. 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
   ```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

You can now update the hosts.

3.4. UPDATING THE HOSTS

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager.

NOTE

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

IMPORTANT

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

Prerequisites

- 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.
- Ensure that the cluster contains more than one host before performing an update. Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve for its hosts to perform maintenance. Otherwise, the virtual machine migration operation will hang and fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed must be shut down before updating the host.

IMPORTANT

RHVH 4.0 hosts cannot be updated with Red Hat Virtualization Manager 4.2. They must be updated manually from the command line:

```
# yum update redhat-virtualization-host-image-update
```

This limitation applies only to RHVH 4.0. Other RHVH versions and all RHEL hosts can be upgraded using Red Hat Virtualization Manager 4.2.

Procedure

1. Ensure that the correct repositories are enabled (to view a list of currently enabled repositories, type **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-2.9-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**.

   Click the **Events and alerts notification** icon (🔔) 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 will be migrated according to their migration policy. If migration is disabled for any virtual machines, you will be 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.

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. See Section A.3, “Updating the Hosts” for more information on updating hosts.

Procedure

1. Click **Compute → Clusters** and select the cluster to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Cluster Compatibility Version** confirmation window.
5. Click **OK** to confirm.

IMPORTANT

An error message may 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.

After you update the cluster’s compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by restarting them from within the Manager, or using the REST API, instead of within the guest operating system. Virtual machines will continue to run in the previous cluster compatibility level until they are restarted. Those virtual machines that require a restart are marked with the pending changes icon (⚠). You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview; you must first commit or undo the preview.

The self-hosted engine virtual machine does not need to be restarted.

Once you have updated the compatibility version of all clusters in a data center, you can then change the compatibility version of the data center itself.

3.6. 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 that the data center is intended to be compatible with. 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 all the clusters in your data center to a level that supports your desired compatibility level.

Procedure

1. Click **Compute → Data Centers** and select the data center to change.

2. Click **Edit**.

3. Change the **Compatibility Version** to the desired value.

4. Click **OK** to open the **Change Data Center Compatibility Version** confirmation window.

5. Click **OK** to confirm.

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

Red Hat Virtualization 4.2 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed 4.2 systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for upgraded systems one of the following is recommended:

- 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 SSL 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 4. UPGRADING FROM 4.1 TO RED HAT VIRTUALIZATION 4.2

Upgrading your environment from 4.1 to 4.2 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 hosts
4. Update the compatibility version of the clusters
5. Update the compatibility version of the data centers
6. Replace SHA-1 certificates with SHA-256 certificates
7. If you installed the technology preview version of Open Virtual Network (OVN) in 4.1, update the OVN provider's networking plugin

4.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

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

Procedure

1. On the Red Hat Virtualization Manager machine, check if updated packages are available:

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

2. Update the setup packages:

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

3. Update the Red Hat Virtualization Manager. 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
```

> **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 may 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.

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

```
# yum update
```

IMPORTANT

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

4.2. 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 will attempt 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. 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-2.9-rpms
```

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

2. Update the setup packages:

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

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

```
# engine-setup
```

NOTE

If you changed the default trust keystore password, you might get a keystore certificate error. If so, update the configuration to reflect the correct password. For more information, see *RHV 4.2 - Failed to import provider certificate into the external provider keystore*

4. 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
```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

You can now update the hosts.

4.3. UPDATING THE HOSTS

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager.

NOTE

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

IMPORTANT

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

Prerequisites

- 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.
- Ensure that the cluster contains more than one host before performing an update. Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve for its hosts to perform maintenance. Otherwise, the virtual machine migration operation will hang and fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed 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, type **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-2.9-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**.

   Click the **Events and alerts notification** icon (🔔) 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 will be migrated according to their migration policy. If migration is disabled for any virtual machines, you will be 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.

4.4. 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. See Section A.3, "Updating the Hosts" for more information on updating hosts.

Procedure

1. Click **Compute → Clusters** and select the cluster to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Cluster Compatibility Version** confirmation window.
5. Click **OK** to confirm.

IMPORTANT

An error message may 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.

After you update the cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by restarting them from within the Manager, or using the REST API, instead of within the guest operating system. Virtual machines will continue to run in the previous cluster compatibility level until they are restarted. Those virtual machines that require a restart are marked with the pending changes icon (⚠). You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview; you must first commit or undo the preview.

The self-hosted engine virtual machine does not need to be restarted.

Once you have updated the compatibility version of all clusters in a data center, you can then change the compatibility version of the data center itself.

4.5. 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 that the data center is intended to be compatible with. 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 all the clusters in your data center to a level that supports your desired compatibility level.

Procedure

1. Click **Compute → Data Centers** and select the data center to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Data Center Compatibility Version** confirmation window.
5. Click **OK** to confirm.

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

Red Hat Virtualization 4.2 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed 4.2 systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for upgraded systems one of the following is recommended:

- 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 SSL 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**.

4.7. 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**.

PART II. UPGRADING A REMOTE DATABASE ENVIRONMENT

CHAPTER 5. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 3.6 TO RED HAT VIRTUALIZATION 4.2

You cannot upgrade the Manager directly from 3.6 to 4.2. You must upgrade your environment in the following sequence:

1. Update the 3.6 Manager to the latest version of 3.6
2. Upgrade the Manager 3.6 to 4.0
3. Upgrade the Manager from 4.0 to 4.1
4. Upgrade the database from PostgreSQL 9.2 to 9.5
5. Upgrade the Manager from 4.1 to 4.2
6. Upgrade the hosts

> **NOTE**
>
> If you are upgrading RHEV-H hosts that use local storage, see Appendix C, *Upgrading from RHEV-H 3.6 to RHVH 4.2 While Preserving Local Storage* .

7. Update the compatibility version of the clusters
8. Update the compatibility version of the data centers
9. If you backed up an ISO storage domain that was hosted on the 3.6 Manager, restore the ISO domain in the upgraded environment
10. Replace SHA-1 certificates with SHA-256 certificates

5.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

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

Procedure

1. On the Red Hat Virtualization Manager machine, check if updated packages are available:

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

2. Update the setup packages:

```
# yum update rhevm-setup
```

3. Update the Red Hat Virtualization Manager. 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
```

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 may 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.

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

```
# yum update
```

IMPORTANT

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

5.2. UPGRADING THE MANAGER FROM 3.6 TO 4.0

In Red Hat Enterprise Virtualization 3.6, the Manager runs on Red Hat Enterprise Linux 6. An in-place upgrade of the Manager machine to Red Hat Enterprise Linux 7 is not supported. To upgrade from 3.6 to 4.0, you must install a new 4.0 Manager on Red Hat Enterprise Linux 7, and restore a backup of the 3.6 Manager database on the new Manager.

If any optional extension packages, such as **ovirt-engine-extension-aaa-ldap**, **ovirt-engine-extension-aaa-misc**, or **ovirt-engine-extension-logger-log4j** are installed on Red Hat Enterprise Virtualization Manager 3.6, they must be installed on the upgraded Manager before running **engine-setup**. The settings for these package extensions are not migrated as part of the upgrade. You can copy the configuration files to the same device or machine as the 3.6 Manager backup file.

NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 3.6 before attempting the procedure.

- Directory servers configured using the domain management tool are not supported after Red Hat Enterprise Virtualization 3.6. If your directory servers are configured using the domain management tool, migrate to the new extension-based provider before backing up the environment. See Migrating from the Legacy Provider to the New Extension-Based Provider in the *Red Hat Enterprise Virtualization 3.6 Administration Guide* for more information.

Procedure

Procedure

1. On the 3.6 Manager, back up the environment:

   ```
   # engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
   ```

2. Copy the backup file to a suitable device or machine.

3. If the ISO storage domain is hosted on the Manager machine, back up the contents of **/var/lib/exports/iso**:

   ```
   # cd /var/lib/exports/iso
   # tar zcf iso_domain.tar.gz UUID
   ```

   You will restore the ISO storage backup file after the upgrade.

4. Install Red Hat Enterprise Linux 7. See the *Red Hat Enterprise Linux Installation Guide* .
   If you are installing RHEL 7 on a new machine, you must configure it to have the same fully qualified domain name as the 3.6 Manager machine, and update your DNS so that the FQDN correlates to the IP address of the new machine.

5. Install the Red Hat Virtualization 4.0 packages:

   a. Register your system with the Content Delivery Network, entering your Customer Portal user name and password when prompted:

      ```
      # subscription-manager register
      ```

   b. Find the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscription pools and record the pool IDs:

      ```
      # subscription-manager list --available
      ```

   c. Use the pool IDs to attach the entitlements to the system:

      ```
      # subscription-manager attach --pool=pool_id
      ```

   d. Configure the repositories:

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

   e. Ensure all packages are up to date:

      ```
      # yum update
      ```

   f. Install the **rhevm** package and dependencies:

      ```
      # yum install rhevm
      ```

6. Copy the backup file to the 4.0 Manager machine and restore the backup:

```
# engine-backup --mode=restore --file=backup.bck --log=restore.log \
   --provision-db --provision-dwh-db --restore-permissions
```

NOTE

If the backup contained grants for extra database users, this command will create the extra users with random passwords. You must change these passwords manually if the extra users require access to the restored system. See https://access.redhat.com/articles/2686731.

NOTE

Use the **--provision-dwh-db** option if the backup contains Data Warehouse data.

Red Hat Enterprise Virtualization Reports has been deprecated in Red Hat Virtualization 4.0 and will not be restored. See BZ#1340810 for more information.

7. Install optional extension packages if they were installed on the 3.6 Manager machine:

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc ovirt-engine-extension-logger-log4j
```

NOTE

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

8. Decommission the 3.6 Manager machine if you are using a different machine for the 4.0 Manager.

9. Run **engine-setup** to configure the Manager:

```
# engine-setup
```

NOTE

If you use external CA to sign HTTPS certificates, follow the steps in Replacing the Red Hat Virtualization Manager SSL Certificate in the *Administration Guide* to log in to the Administration Portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works.

5.3. 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 will attempt 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. 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.

2. Update the setup packages:

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

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

```
# engine-setup
```

4. 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
```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

5.4. UPGRADING REMOTE DATABASES FROM PG 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, and you can skip this section and proceed to the next step. 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-ossp** 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-ossp";
   ```

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 the **postgresql.conf** file:

```
# vi /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
```

The remote databases have been upgraded.

5.5. 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 will attempt 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. 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-2.9-rpms
```

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

2. Update the setup packages:

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

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

```
# engine-setup
```

NOTE

If you changed the default trust keystore password, you might get a keystore certificate error. If so, update the configuration to reflect the correct password. For more information, see *RHV 4.2 - Failed to import provider certificate into the external provider keystore*

4. 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
```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

7. If Data Warehouse is installed on a separate machine, log in to that machine and restart the **ovirt-engine-dwhd** service:

```
# systemctl restart ovirt-engine-dwhd
```

You can now update the hosts.

5.6. UPDATING THE HOSTS

IMPORTANT

Use this procedure to update Red Hat Enterprise Linux hosts or Red Hat Virtualization Hosts (RHVH).

Legacy Red Hat Enterprise Virtualization Hypervisors (RHEV-H) are not supported in Red Hat Virtualization; you must reinstall them with RHVH. See Installing Red Hat Virtualization Host in the *Installation Guide*. If you need to preserve local storage on the host, see Appendix C, *Upgrading from RHEV-H 3.6 to RHVH 4.2 While Preserving Local Storage*.

If you are not sure whether you are using RHEV-H or RHVH, type **imgbase check**. If the command fails, the host is RHEV-H. If it succeeds, the host is RHVH.

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager.

NOTE

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

IMPORTANT

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

Prerequisites

- 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.
- Ensure that the cluster contains more than one host before performing an update. Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve for its hosts to perform maintenance. Otherwise, the virtual machine migration operation will hang and fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed must be shut down before updating the host.

Procedure

1. If your Red Hat Enterprise Linux hosts are locked to version 7.3, as described in https://access.redhat.com/solutions/3194482, set them to the general RHEL 7 version before updating (to view the version number, type **subscription-manager release --show**):

   ```
   # subscription-manager release --set=7Server
   ```

2. Disable your current repositories:

   ```
   # subscription-manager repos --disable='*'
   ```

3. Ensure that the correct repositories are enabled (to view a list of currently enabled repositories, type **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-2.9-rpms
     ```

4. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.

5. Click **Installation** → **Check for Upgrade** and click **OK**.

   Click the **Events and alerts notification** icon (🔔) and expand the **Events** section to see the result.

6. If an update is available, click **Installation → Upgrade**.

7. Click **OK** to update the host. Running virtual machines will be migrated according to their migration policy. If migration is disabled for any virtual machines, you will be 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.

5.7. 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. See Section A.3, "Updating the Hosts" for more information on updating hosts.

Procedure

1. Click **Compute → Clusters** and select the cluster to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Cluster Compatibility Version** confirmation window.
5. Click **OK** to confirm.

IMPORTANT

An error message may 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.

After you update the cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by restarting them from within the Manager, or using the REST API, instead of within the guest operating system. Virtual machines will continue to run in the previous cluster compatibility level until they are restarted. Those virtual machines that require a restart are marked with the pending changes icon (⚠). You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview; you must first commit or undo the preview.

The self-hosted engine virtual machine does not need to be restarted.

Once you have updated the compatibility version of all clusters in a data center, you can then change the compatibility version of the data center itself.

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 that the data center is intended to be compatible with. 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 all the clusters in your data center to a level that supports your desired compatibility level.

Procedure

1. Click **Compute → Data Centers** and select the data center to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Data Center Compatibility Version** confirmation window.
5. Click **OK** to confirm.

5.9. MIGRATING THE ISO DOMAIN FROM 3.6

Migrate the ISO domain from 3.6 to the current version of Red Hat Virtualization, using the **iso_domain.tar.gz** backup file that you created during the upgrade from 3.6 to 4.0.

IMPORTANT

The new directory for the ISO domain must not be on the Manager machine.

NOTE

The ISO domain is deprecated in Red Hat Virtualization 4.2, and will be removed in a future version. Red Hat recommends uploading ISO images to a data storage domain. See Uploading Images to a Data Storage Domain in the *Administration Guide*.

1. Create an export directory on the storage server and set its permissions:

   ```
   # mkdir -p /var/lib/exports/iso
   # chown -R 36:36 /var/lib/exports/
   ```

2. Extract the ISO domain backup to this directory:

   ```
   # cd /var/lib/exports/iso
   # tar zxf iso_domain.tar.gz
   ```

3. Set the SELinux context for the files in the export directory:

   ```
   # chcon -R system_u:object_r:public_content_rw_t:s0 /var/lib/exports/iso/
   ```

4. Create **/etc/exports.d/ovirt-engine-iso-domain.exports** with the following line:

   ```
   /var/lib/exports/iso  *(rw)
   ```

5. Edit the following lines in **/etc/sysconfig/nfs**:

   ```
   RPCMOUNTDOPTS="-p 892"
   (..snip..)
   STATDARGS="-p 662 -o 2020"
   (..snip..)
   LOCKD_UDPPORT=32769
   LOCKD_TCPPORT=32803
   RPCRQUOTAOPTS="-p 875"
   ```

6. Enable the **nfs** service:

   ```
   # systemctl enable nfs
   # systemctl start nfs
   ```

7. Allow services and ports with **firewalld**:

   ```
   # firewall-cmd --add-service={nfs,rpc-bind}
   # firewall-cmd --add-service={nfs,rpc-bind} --permanent
   # firewall-cmd --add-port=
   {32769/udp,32803/tcp,662/tcp,662/udp,875/tcp,875/udp,892/tcp,892/udp}
   # firewall-cmd --add-port=
   {32769/udp,32803/tcp,662/tcp,662/udp,875/tcp,875/udp,892/tcp,892/udp} --permanent
   ```

8. In the Administration Portal, update the ISO domain’s storage path:

   a. Click **Storage** → **Domains**.

   b. Click the ISO domain’s name to go to the details view.

c. Click the **Data Center** tab and click **Maintenance**.

d. When the ISO domain is in maintenance mode, click **Manage Domain**.

e. Change the **Export Path** to point to the new directory, for example: *storage.example.com*:/var/lib/exports/iso

f. Click **OK**.

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

Red Hat Virtualization 4.2 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed 4.2 systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for upgraded systems one of the following is recommended:

- 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 SSL 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 4.0 TO RED HAT VIRTUALIZATION 4.2

You cannot upgrade the Manager directly from 4.0 to 4.2. You must upgrade your environment in the following sequence:

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. Upgrade the hosts
6. Update the compatibility version of the clusters
7. Update the compatibility version of the data centers
8. Replace SHA-1 certificates with SHA-256 certificates

6.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

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

Procedure

1. On the Red Hat Virtualization Manager machine, check if updated packages are available:

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

2. Update the setup packages:

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

3. Update the Red Hat Virtualization Manager. 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
   ```

   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 may 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.

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

```
# yum update
```

IMPORTANT

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

6.2. 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 will attempt 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. 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.

2. Update the setup packages:

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

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

```
# engine-setup
```

4. 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
```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

6.3. UPGRADING REMOTE DATABASES FROM PG 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, and you can skip this section and proceed to the next step. 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-ossp** 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-ossp";
```

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 the **postgresql.conf** file:

```
# vi /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
```

The remote databases have been upgraded.

6.4. 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 will attempt 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. 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-2.9-rpms
```

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

2. Update the setup packages:

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

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

```
# engine-setup
```

NOTE

If you changed the default trust keystore password, you might get a keystore certificate error. If so, update the configuration to reflect the correct password. For more information, see *RHV 4.2 - Failed to import provider certificate into the external provider keystore*

4. 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
```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

7. If Data Warehouse is installed on a separate machine, log in to that machine and restart the **ovirt-engine-dwhd** service:

```
# systemctl restart ovirt-engine-dwhd
```

You can now update the hosts.

6.5. UPDATING THE HOSTS

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager.

NOTE

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

IMPORTANT

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

Prerequisites

- 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.
- Ensure that the cluster contains more than one host before performing an update. Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve for its hosts to perform maintenance. Otherwise, the virtual machine migration operation will hang and fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed must be shut down before updating the host.

IMPORTANT

RHVH 4.0 hosts cannot be updated with Red Hat Virtualization Manager 4.2. They must be updated manually from the command line:

```
# yum update redhat-virtualization-host-image-update
```

This limitation applies only to RHVH 4.0. Other RHVH versions and all RHEL hosts can be upgraded using Red Hat Virtualization Manager 4.2.

Procedure

1. Ensure that the correct repositories are enabled (to view a list of currently enabled repositories, type **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-2.9-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**.

   Click the **Events and alerts notification** icon (🔔) 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 will be migrated according to their migration policy. If migration is disabled for any virtual machines, you will be 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.

6.6. 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. See Section A.3, "Updating the Hosts" for more information on updating hosts.

Procedure

1. Click **Compute → Clusters** and select the cluster to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Cluster Compatibility Version** confirmation window.
5. Click **OK** to confirm.

IMPORTANT

An error message may 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.

After you update the cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by restarting them from within the Manager, or using the REST API, instead of within the guest operating system. Virtual machines will continue to run in the previous cluster compatibility level until they are restarted. Those virtual machines that require a restart are marked with the pending changes icon (⚠). You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview; you must first commit or undo the preview.

The self-hosted engine virtual machine does not need to be restarted.

Once you have updated the compatibility version of all clusters in a data center, you can then change the compatibility version of the data center itself.

6.7. 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 that the data center is intended to be compatible with. 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 all the clusters in your data center to a level that supports your desired compatibility level.

Procedure

1. Click **Compute → Data Centers** and select the data center to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Data Center Compatibility Version** confirmation window.
5. Click **OK** to confirm.

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

Red Hat Virtualization 4.2 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed 4.2 systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for upgraded systems one of the following is recommended:

- 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 SSL 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 7. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.1 TO RED HAT VIRTUALIZATION 4.2

Upgrading your environment from 4.1 to 4.2 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 hosts
5. Update the compatibility version of the clusters
6. Update the compatibility version of the data centers
7. Replace SHA-1 certificates with SHA-256 certificates
8. If you installed the technology preview version of Open Virtual Network (OVN) in 4.1, update the OVN provider’s networking plugin

7.1. UPGRADING REMOTE DATABASES FROM PG 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, and you can skip this section and proceed to the next step. 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-ossp** 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-ossp";
```

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 the **postgresql.conf** file:

```
# vi /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
```

The remote databases have been upgraded.

7.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

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

Procedure

1. On the Red Hat Virtualization Manager machine, check if updated packages are available:

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

2. Update the setup packages:

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

3. Update the Red Hat Virtualization Manager. 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
```

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 may 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.

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

```
# yum update
```

IMPORTANT

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

7.3. 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 will attempt 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. 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-2.9-rpms
```

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

2. Update the setup packages:

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

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

```
# engine-setup
```

   NOTE

   If you changed the default trust keystore password, you might get a keystore certificate error. If so, update the configuration to reflect the correct password. For more information, see *RHV 4.2 - Failed to import provider certificate into the external provider keystore*

4. 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
```

5. Update the base operating system:

```
# yum update
```

6. Reboot the machine.

7. If Data Warehouse is installed on a separate machine, log in to that machine and restart the **ovirt-engine-dwhd** service:

```
# systemctl restart ovirt-engine-dwhd
```

You can now update the hosts.

7.4. UPDATING THE HOSTS

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager.

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

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

Prerequisites

- 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.
- Ensure that the cluster contains more than one host before performing an update. Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve for its hosts to perform maintenance. Otherwise, the virtual machine migration operation will hang and fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed 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, type **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-2.9-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**.

   Click the **Events and alerts notification** icon (🔔) 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 will be migrated according to their migration policy. If migration is disabled for any virtual machines, you will be 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.

7.5. 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. See Section A.3, "Updating the Hosts" for more information on updating hosts.

Procedure

1. Click **Compute → Clusters** and select the cluster to change.

2. Click **Edit**.

3. Change the **Compatibility Version** to the desired value.

4. Click **OK** to open the **Change Cluster Compatibility Version** confirmation window.

5. Click **OK** to confirm.

> **IMPORTANT**
>
> An error message may 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.

After you update the cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by restarting them from within the Manager, or using the REST API, instead of within the guest operating system. Virtual machines will continue to run in the previous cluster compatibility level until they are restarted. Those virtual machines that require a restart are marked with the pending changes icon (⚠). You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview; you must first commit or undo the preview.

The self-hosted engine virtual machine does not need to be restarted.

Once you have updated the compatibility version of all clusters in a data center, you can then change the compatibility version of the data center itself.

7.6. 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 that the data center is intended to be compatible with. 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 all the clusters in your data center to a level that supports your desired compatibility level.

Procedure

1. Click **Compute → Data Centers** and select the data center to change.
2. Click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK** to open the **Change Data Center Compatibility Version** confirmation window.
5. Click **OK** to confirm.

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

Red Hat Virtualization 4.2 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed 4.2 systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures. However, for upgraded systems one of the following is recommended:

- 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 SSL 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**.

7.8. 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**.

APPENDIX A. UPDATES BETWEEN MINOR RELEASES

To update from your current version of 4.2 to the latest version of 4.2, 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
   ```

A.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

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

Procedure

1. On the Red Hat Virtualization Manager machine, check if updated packages are available:

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

   > **NOTE**
   >
   > If updates are expected, but not available, enable the required repositories. See Enabling the Red Hat Virtualization Manager Repositories in the *Installation Guide*.

2. Update the setup packages:

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

3. Update the Red Hat Virtualization Manager. 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
   ```

   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 may 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.

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

   ```
   # yum update
   ```

   IMPORTANT

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

NOTE

If the update from RHV 4.2.7 to RHV 4.2.8 fails with a message indicating a dependency error with an **eap7-jboss-server-migration-wildfly** package:

1. Check if all the required repositories are enabled.
2. Update the **eap7-jboss-server-migration-wildfly** packages installed on the Manager:

   ```
   # yum update eap7-jboss-server-migration-wildfly*
   ```

3. Run **engine-setup** again.

A.3. UPDATING THE HOSTS

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager.

NOTE

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

IMPORTANT

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

Prerequisites

- 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.
- Ensure that the cluster contains more than one host before performing an update. Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve for its hosts to perform maintenance. Otherwise, the virtual machine migration operation will hang and fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed 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, type **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-2.9-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**.

    Click the **Events and alerts notification** icon (🔔) 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 will be migrated according to their migration policy. If migration is disabled for any virtual machines, you will be 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 Manager; however, you can also update the hosts using **yum update**.

A.4. 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.

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

Prerequisites

- If migration is enabled at cluster level, virtual machines are automatically migrated to another host in the cluster; as a result, it is recommended that host updates are performed at a time when the host's usage is relatively low.
- Ensure that the cluster contains more than one host before performing an update. Do not attempt to update all the hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- Ensure that the cluster to which the host belongs has sufficient memory reserve in order for its hosts to perform maintenance. If a cluster lacks sufficient memory, the virtual machine migration operation will hang and then fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before updating the host.
- You cannot migrate a virtual machine using a vGPU to a different host. Virtual machines with vGPUs installed 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-2.9-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 may 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] for information on updating the Manager between minor versions. See xref:Red_Hat_Virtualization_Upgrade_Overview[for information on upgrading between major versions.

APPENDIX C. UPGRADING FROM RHEV-H 3.6 TO RHVH 4.2 WHILE PRESERVING LOCAL STORAGE

Environments with local storage cannot migrate virtual machines to a host in another cluster (for example when upgrading to version 4.2) because the local storage is not shared with other storage domains. To upgrade RHEV-H 3.6 hosts that have a local storage domain, reinstall the host while preserving the local storage, create a new local storage domain in the 4.2 environment, and import the previous local storage into the new domain. Follow the procedure in Upgrading to RHVH While Preserving Local Storage in the *Red Hat Virtualization 4.0 Upgrade Guide* , but install a RHVH 4.2 host instead of a 4.0 host.

IMPORTANT

An exclamation mark icon appears next to the name of the virtual machine if a MAC address conflict is detected when importing the virtual machines into the 4.2 storage domain. Move the cursor over the icon to view a tooltip displaying the type of error that occurred.

Select the **Reassign Bad MACs** check box to reassign new MAC addresses to all problematic virtual machines. See Importing Virtual Machines from Imported Data Storage Domains in the *Administration Guide* for more information.

APPENDIX D. UPGRADING TO RED HAT VIRTUALIZATION MANAGER 4.2 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, "Manually Updating Hosts" 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**.