Red Hat Virtualization 4.1

Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Red Hat Virtualization 4.1 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. UPDATING THE RED HAT VIRTUALIZATION ENVIRONMENT

1.1. UPDATE OVERVIEW

This guide covers updating your Red Hat Virtualization environment between minor releases, and upgrading to the next major version. Always update to the latest minor version of your current Red Hat Virtualization Manager version before you upgrade to the next major version.

For interactive upgrade instructions, you can also use the RHEV Upgrade Helper available at https://access.redhat.com/labs/rhevupgradehelper/. 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.

Upgrading the Red Hat Virtualization Manager involves the following key steps:

- Subscribe to the appropriate entitlements

- Update the system

- Run **engine-setup**

- Remove repositories that are no longer required

Updating RHVH and RHEL hosts:

Hosts can be upgraded directly from the Red Hat Virtualization Manager, which checks for and notifies you of available host updates.

Update cluster and data center compatibility level

The command used to perform the upgrade itself is **engine-setup**, which provides an interactive interface. While the upgrade is in progress, virtualization hosts and the virtual machines running on those virtualization hosts continue to operate independently. When the upgrade is complete, you can then upgrade your hosts to the latest versions of Red Hat Enterprise Linux or Red Hat Virtualization Host.

CHAPTER 2. UPDATES BETWEEN MINOR RELEASES

2.1. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Updates to the Red Hat Virtualization Manager are released via the Content Delivery Network. Before installing an update from the Content Delivery Network, ensure you read the advisory text associated with it and the latest version of the *Red Hat Virtualization Manager Release Notes* and *Red Hat Virtualization Technical Notes* on the Customer Portal.

Procedure 2.1. Updating Red Hat Virtualization Manager

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

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

2. ○ If there are no updates are available, the command will output the text **No upgrade**:

   ```
   # engine-upgrade-check
   VERB: queue package ovirt-engine-setup for update
   VERB: package ovirt-engine-setup queued
   VERB: Building transaction
   VERB: Empty transaction
   VERB: Transaction Summary:
   No upgrade
   ```

   NOTE

   If updates are expected, but not available, ensure that the required repositories are enabled. See Subscribing to the Required Entitlements in the *Installation Guide*.

   ○ If updates are available, the command will list the packages to be updated:

   ```
   # engine-upgrade-check
   VERB: queue package ovirt-engine-setup for update
   VERB: package ovirt-engine-setup queued
   VERB: Building transaction
   VERB: Transaction built
   VERB: Transaction Summary:
   VERB:    updated   - ovirt-engine-lib-3.3.2-0.50.el6ev.noarch
   VERB:    update    - ovirt-engine-lib-3.4.0-0.13.el6ev.noarch
   VERB:    updated   - ovirt-engine-setup-3.3.2-0.50.el6ev.noarch
   VERB:    update    - ovirt-engine-setup-3.4.0-0.13.el6ev.noarch
   VERB:    install   - ovirt-engine-setup-base-3.4.0-0.13.el6ev.noarch
   VERB:    install   - ovirt-engine-setup-plugin-ovirt-engine-3.4.0-0.13.el6ev.noarch
   VERB:    updated   - ovirt-engine-setup-plugins-3.3.1-1.el6ev.noarch
   VERB:    update    - ovirt-engine-setup-plugins-3.4.0-0.5.el6ev.noarch
   Upgrade available

   Upgrade available
   ```

3. Update the setup packages:

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

4. Update the Red Hat Virtualization Manager. By running **engine-setup**, the script will prompt you with some configuration questions like updating the firewall rules, updating PKI certificates, and backing up the Data Warehouse database. The script will then go through the process of stopping the **ovirt-engine** service, downloading and installing the updated packages, backing up and updating the database, performing post-installation configuration, and starting the **ovirt-engine** service.

> **NOTE**
>
> The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values that were 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**.

```
# engine-setup
```
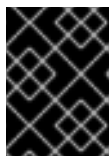
> **IMPORTANT**
>
> The update process may take some time; allow time for the update process to complete and do not stop the process once initiated.

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

```
# yum update
```
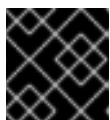
> **IMPORTANT**
>
> If any kernel packages were updated, reboot the system to complete the update.

2.2. UPDATING HOSTS

Use the host upgrade manager to update individual hosts directly from the Red Hat Virtualization Manager. The upgrade manager checks for and notifies you of available host updates, and reduces the time required by automating the process of putting the host into maintenance mode, updating packages, and bringing the host back up. On large deployments with many hosts, this automated process can save a significant amount of time.

> **NOTE**
>
> The upgrade manager checks only hosts whose status is **Up** or **Non-operational**. Hosts in **Maintenance** are not checked.

On Red Hat Enterprise Linux hosts, the upgrade manager checks for updates to Red Hat Virtualization packages by default. You can specify additional packages for the upgrade manager to monitor for

updates using the system configuration value **UserPackageNamesForCheckUpdate**. Run the **engine-config** command on the Manager machine. For example:

```
# engine-config -m UserPackageNamesForCheckUpdate=vdsm-hook-ethtool-options
```

> **WARNING**
>
> For other updates, such as security fixes for the operating system, you must manually update Red Hat Enterprise Linux hosts with **yum update** as shown in Section 2.3, "Manually Updating Hosts".

On Red Hat Virtualization Host (RHVH), the upgrade manager uses **yum check-update** to automatically check for updates to the RHVH image, provided that you registered the host and enabled the **Red Hat Virtualization Host 7** repository when installing the host. This repository contains the **redhat-virtualization-host-image-update** package, which is responsible for updating the image. See Installing Red Hat Virtualization Host in the *Installation Guide* for more details.

As the RHVH image as a whole is updated, rather than individual packages, manually running **yum update** for other packages is not necessary. Modified content in only the /**etc** and /**var** directories is preserved during an update. Modified data in other paths is completely replaced during an update.

The upgrade manager checks for updates every 24 hours by default. You can change this setting using the **HostPackagesUpdateTimeInHours** configuration value. Run the **engine-config** command on the Manager machine. For example:

```
# engine-config -s HostPackagesUpdateTimeInHours=48
```

You can disable periodic automatic host upgrade checks, using the **HostPackagesUpdateTimeInHours** configuration value. Automatic upgrade checks are not always needed, for example, when managing the hosts with Satellite. Run the **engine-config** command on the Manager machine:

```
# engine-config -s HostPackagesUpdateTimeInHours=0
```

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.
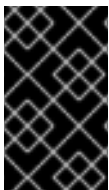
> **IMPORTANT**
>
> Ensure that the cluster contains more than one host before performing an update. Do not attempt to update all the hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.

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.

IMPORTANT

If updating from RHVH 3.6, ensure that you disable the 3.6 repository, and enable the 4.1 repository on the host being updated:

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

Procedure 2.2. Updating Red Hat Enterprise Linux hosts and Red Hat Virtualization Host

1. Click the **Hosts** tab and select the host to be updated.

    ○ If the host requires updating, an alert message under **Action Items** and an icon next to the host's name indicate that a new version is available.

    ○ If the host does not require updating, no alert message or icon is displayed and no further action is required.

2. Click **Installation → Check for Upgrade** to open the **Upgrade Host** confirmation window.

3. Click **OK** to begin the upgrade check.

4. If you want to upgrade the host, click **Installation → Upgrade** to open the **Upgrade Host** confirmation window.

5. Click **OK** to update the host. The details of the host are updated in the **Hosts** tab, and the status will transition through these stages:

    ○ **Maintenance**

    ○ **Installing**

    ○ **Up**

Once successfully updated, the host displays a status of **Up**. Any virtual machines that were migrated off the host are, at this point, able to be migrated back to it. Repeat the update procedure for each host in the Red Hat Virtualization environment.

NOTE

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

2.3. MANUALLY UPDATING HOSTS

Red Hat Enterprise Linux hosts use the **yum** command in the same way as regular Red Hat Enterprise Linux systems. Red Hat Virtualization Host (RHVH) can use the **yum** command for updates, and to install additional packages and have them persist after an upgrade. It is highly recommended that you use **yum** to update your systems regularly, to ensure timely application of security and bug fixes. Updating a host includes stopping and restarting the host. 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.

> **IMPORTANT**
>
> 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.

The cluster to which the host belongs must have sufficient memory reserve in order for its hosts to perform maintenance. Moving a host with live virtual machines to maintenance in a cluster that lacks sufficient memory causes any virtual machine migration operations to hang and then fail. You can reduce the memory usage of this operation by shutting down some or all virtual machines before moving the host to maintenance.

> **IMPORTANT**
>
> If updating from RHVH 3.6, ensure that you disable the 3.6 repository, and enable the 4.1 repository on the host being updated:
>
> ```
> # subscription-manager repos --disable=rhel-7-server-rhevh-rpms
> # subscription-manager repos --enable=rhel-7-server-rhvh-4-rpms
> ```

Procedure 2.3. Manually Updating Hosts

1. From the Administration Portal, click the **Hosts** tab and select the host to be updated.

2. Click **Management → Maintenance** to place the host into maintenance mode.

3.
   - On a Red Hat Enterprise Linux host, log in to the host machine and run the following command:

     ```
     # yum update
     ```

   - On a Red Hat Virtualization Host, log in to the Cockpit user interface, click **Terminal**, and run the following command:

     ```
     # yum update
     ```

4. Restart the host to ensure all updates are correctly applied.
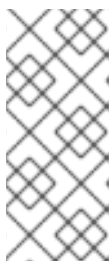
> **NOTE**
>
> Check the imgbased logs to see if any additional package updates have failed for a Red Hat Virtualization Host. If some packages were not successfully reinstalled after the update, check that the packages are listed in **/var/imgbased/persisted-rpms**. Add any missing packages then run **rpm -Uvh /var/imgbased/persisted-rpms/***.

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

2.4. RECOVERING FROM FAILED NIST–800 UPGRADE

Red Hat Virtualization Host (RHVH) supports NIST 800-53 partitioning by default, for greater security. The NIST 800-53 partition structure places each of the following directories in its own partition: /, **/tmp**, **/home**, **/var**, and **/var/log/audit**.

If you attempt to move from a NIST 800-compatible version to a non-NIST-800 version because of an upgrade failure or to resolve an issue, future upgrades will fail because the logical volumes created by the NIST-800 partitioning cannot be removed automatically without loss of data. The relevant logs must be backed up and the logical volumes must be removed manually.

Procedure 2.4. Removing NIST-800 Partitions

1. Back up the logs located in **/var/log** and **/var/log/audit**.

2. Remove the following logical volumes manually:

   - **/tmp**

   - **/home**

   - **/var**

   - **/var/log/audit**. The **lvm lvs** command may show this logical volume as **rhvh_var_log_audit**.

   See Removing Logical Volumes in the *Logical Volume Manager Administration* for details.

2.5. UPDATING THE SELF-HOSTED ENGINE MANAGER

To update a self-hosted engine, see Updating the Self-Hosted Engine Manager Between Minor Releases in the *Self-Hosted Engine Guide*.

CHAPTER 3. UPGRADING TO RED HAT VIRTUALIZATION 4.1

3.1. UPGRADE CONSIDERATIONS

The following is a list of key considerations that must be made when planning your upgrade.

> **IMPORTANT**
>
> **Upgrading Red Hat Virtualization Manager to version 4.1 can only be performed from version 4.0**
>
> > To upgrade the Manager from a version earlier than 4.0 to 4.1, you must sequentially upgrade to later versions of the Manager before upgrading to the latest version. In other words, the Manager upgrades must be stepped. For example, if you are using 3.6, you must upgrade to the next version (4.0) first. See Upgrading to Red Hat Virtualization 4.0 in the *Upgrade Guide* for Red Hat Virtualization 4.0 for instructions to upgrade 3.6 to 4.0.
> >
> > If you are using 4.0, you must update your installation to the latest 4.0 minor release, before upgrading to 4.1. See Updates between Minor Releases for instructions to update to the latest 4.0 minor version.
> >
> > The host upgrade procedure does not need to be stepped.
>
> **Downgrading is not possible after changing the data center compatibility version to 4.1**
>
> > When you upgrade the data center compatibility version to 4.1, the data domain storage format changes from version 3 to version 4 and cannot be downgraded. Therefore, you cannot attach a data domain from a 4.1 data center to an older data center. However, you can attach a data domain from an older data center to a 4.1 data center, but the storage format will also be upgraded and cannot be reversed.

3.2. UPGRADING TO RED HAT VIRTUALIZATION MANAGER 4.1

The following procedure outlines the process for upgrading Red Hat Virtualization Manager 4.0 to Red Hat Virtualization Manager 4.1 in a standard deployment. See Upgrading a Self-Hosted Engine Environment in the *Self-Hosted Engine Guide* for more information about upgrading the Manager in a Self-hosted Engine deployment.

This procedure assumes that the system on which the Manager is installed is subscribed to the entitlements for receiving Red Hat Virtualization 4.0 packages.

> **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 repositories required by Red Hat Virtualization 4.0 must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

> **IMPORTANT**
>
> Ensure that you are running the latest minor version of Red Hat Virtualization Manager 4.0 before upgrading by running **engine-upgrade-check**. See Section 2.1, "Updating the Red Hat Virtualization Manager" for more information.

Procedure 3.1. Upgrading to Red Hat Virtualization Manager 4.1

1. Enable the Red Hat Virtualization Manager 4.1 and Red Hat Virtualization Tools 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
   ```

2. Update the setup packages:

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

3. Run the following command and follow the prompts to upgrade the Red Hat Virtualization Manager:

   ```
   # engine-setup
   ```

4. Remove or disable the Red Hat Virtualization Manager 4.0 repository to ensure the system does not use any Red Hat Virtualization Manager 4.0 packages:

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

5. Update the base operating system:

   ```
   # yum update
   ```

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

You must now change the cluster and data center compatibility version to 4.1. See Chapter 4, *Post-Upgrade Tasks*.

3.3. UPGRADING TO RHVH WHILE PRESERVING LOCAL STORAGE

Environments with local storage cannot migrate virtual machines to a host in another cluster (for example when upgrading to version 4.1) 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 4.1 environment, and import the previous local storage into the new domain. Follow the procedure in Upgrading to RHVH While Preserving Local Storage in the *Upgrade Guide* for Red Hat Virtualization 4.0, but install a RHVH 4.1 host instead or 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 4.1 storage domain. Mouse 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.

3.4. UPGRADING THE SELF-HOSTED ENGINE

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

CHAPTER 4. POST-UPGRADE TASKS

4.1. 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.
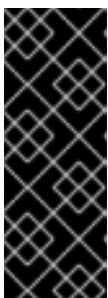
> **IMPORTANT**
>
> To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available. See Section 2.2, "Updating Hosts" for more information on updating hosts.

After you update the cluster compatibility version of the cluster you need to update the cluster compatibility version of all running or suspended virtual machines to ensure that the changes become effective. This is achieved by restarting the virtual machines from within the Manager or REST API call 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 **Next-Run** icon (triangle with an exclamation mark). You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview, you need to first commit or undo the preview.

The self-hosted engine virtual machine does not need to be restarted, see Maintenance and Upgrading Resources in the *Self-Hosted Engine Guide* for more information about upgrading the Self-Hosted Engine environment.

Procedure 4.1. Changing the Cluster Compatibility Version

1. From the Administration Portal, click the **Clusters** tab.

2. Select the cluster to change from the list displayed.

3. Click **Edit**.

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

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

6. 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.

You have updated the compatibility version of the cluster. 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.

4.2. 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 4.2. Changing the Data Center Compatibility Version

1. From the Administration Portal, click the **Data Centers** tab.

2. Select the data center to change from the list displayed.

3. Click **Edit**.

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

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

6. Click **OK** to confirm.

You have updated the compatibility version of the data center.

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

Red Hat Virtualization 4.1 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed 4.1 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:

- Option 1: 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*.

- Option 2: Replace the SHA-1 certificates throughout the system with SHA-256 certificates.

Procedure 4.3. 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. For self-hosted engine environments, log in to one of the self-hosted engine nodes and enable global maintenance:

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

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

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

6. Restart the **httpd** service:

```
# systemctl restart httpd
```

7. For self-hosted engine environments, log in to one of the self-hosted engine nodes and disable global maintenance:

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

8. Connect to the Administration Portal to confirm that the warning no longer appears.

9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **http://*your-manager-fqdn*/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Procedure 4.4. 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. For self-hosted engine environments, log in to one of the self-hosted engine nodes and enable global maintenance:

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

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

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

```
        --password=mypass \
        --subject="${subject}" \
        --keep-key
done
```

8. Restart the following services:

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

9. For self-hosted engine environments, log in to one of the self-hosted engine nodes and disable global maintenance:

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

10. Connect to the Administration Portal to confirm that the warning no longer appears.

11. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **http://** *your-manager-fqdn***/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

12. Enroll the certificates on the hosts. Repeat the following procedure for each host.

    a. In the Administration Portal, click the **Hosts** tab.

    b. Select the host, and click **Management → Maintenance**.

    c. Once the host is in maintenance mode, click **Installation → Enroll Certificate**.

    d. Click **Management → Activate**.

APPENDIX A. UPDATING AN OFFLINE RED HAT VIRTUALIZATION MANAGER

A.1. 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 Section 2.1, "Updating the Red Hat Virtualization Manager" for information on updating the Manager between minor versions. See Section 1.1, "Update Overview" for information on upgrading between major versions.