Red Hat

Red Hat Virtualization 4.2

Self-Hosted Engine Guide

Installing and Maintaining the Red Hat Virtualization Self-Hosted Engine

Last Updated: 2020-06-03

Red Hat Virtualization 4.2 Self-Hosted Engine Guide

Installing and Maintaining the Red Hat Virtualization Self-Hosted Engine

Red Hat Virtualization Documentation Team
Red Hat Customer Content Services
rhev-docs@redhat.com

Legal Notice

Abstract

A comprehensive guide to the self-hosted engine.

Table of Contents

CHAPTER 1. INTRODUCTION

A self-hosted engine is a virtualized environment in which the Red Hat Virtualization Manager, or engine, runs on a virtual machine on the hosts managed by that Manager. The virtual machine is created as part of the host configuration, and the Manager is installed and configured in parallel to the host configuration process. The primary benefit of the self-hosted engine is that it requires less hardware to deploy an instance of Red Hat Virtualization as the Manager runs as a virtual machine, not on physical hardware. Additionally, the Manager is configured to be highly available. If the host running the Manager virtual machine goes into maintenance mode, or fails unexpectedly, the virtual machine migrates automatically to another host in the environment. Hosts that can run the Manager virtual machine are referred to as self-hosted engine nodes. At least two self-hosted engine nodes are required to support the high availability feature.

For the Manager virtual machine installation, a RHV-M Appliance is provided. Manually installing the Manager virtual machine is not supported.

Self-hosted engine deployment is performed through a simplified wizard in the Cockpit user interface, or through the command line using **hosted-engine --deploy**. Cockpit is the preferred installation method.

Table 1.1. Supported OS versions to Deploy Self-Hosted Engine

System Type	Supported Versions
Red Hat Enterprise Linux host	7.5
Red Hat Virtualization Host	7.5
HostedEngine-VM (Manager)	7.5

For hardware requirements, see Host Requirements in the *Planning and Prerequisites Guide*.

IMPORTANT

To avoid potential timing or authentication issues, configure the Network Time Protocol (NTP) on the hosts, Manager, and other servers in the environment to synchronize with the same NTP server. See Configuring NTP Using the chrony Suite and Synchronizing the System Clock with a Remote Server in the *Red Hat Enterprise Linux 7 System Administrator's Guide*.

CHAPTER 2. DEPLOYING THE SELF-HOSTED ENGINE

You can deploy a self-hosted engine from the command line, or through the Cockpit user interface. Cockpit is available by default on Red Hat Virtualization Hosts, and can be installed on Red Hat Enterprise Linux hosts. Both methods use Ansible to automate most of the process.

Self-hosted engine installation uses the RHV-M Appliance to create the Manager virtual machine. The appliance is installed during the deployment process; however, you can install it on the host before starting the deployment if required:

```
# yum install rhvm-appliance
```

IMPORTANT

See Self-Hosted Engine Recommendations in the *Planning and Prerequisites Guide* for specific recommendations about the self-hosted engine environment.

If you plan to use bonded interfaces for high availability or VLANs to separate different types of traffic (for example, for storage or management connections), you should configure them before deployment. See Networking Recommendations in the *Planning and Prerequisites Guide*.

If you want to deploy the self-hosted engine with Red Hat Gluster Storage as part of a Red Hat Hyperconverged Infrastructure (RHHI) environment, see the *Deploying Red Hat Hyperconverged Infrastructure Guide* for more information.

2.1. DEPLOYING THE SELF-HOSTED ENGINE USING COCKPIT

You can deploy a self-hosted engine through Cockpit using a simplified wizard to collect the details of your environment. This is the recommended method.

Cockpit is enabled by default on Red Hat Virtualization Hosts. If you are using a Red Hat Enterprise Linux host, see Installing Cockpit on Red Hat Enterprise Linux Hosts in the *Installation Guide*.

Prerequisites

- A fresh installation of Red Hat Virtualization Host or Red Hat Enterprise Linux 7, with the required repositories enabled. See Installing Red Hat Virtualization Host or Enabling the Red Hat Enterprise Linux Host Repositories in the *Installation Guide*.

- A fully qualified domain name prepared for your Manager and the host. Forward and reverse lookup records must both be set in the DNS.

- A directory of at least 5 GB on the host, for the RHV-M Appliance. The deployment process will check if **/var/tmp** has enough space to extract the appliance files. If not, you can specify a different directory or mount external storage. The VDSM user and KVM group must have read, write, and execute permissions on the directory.

- Prepared storage for a data storage domain dedicated to the Manager virtual machine. This storage domain is created during the self-hosted engine deployment, and must be at least 74 GiB. Highly available storage is recommended. For more information on preparing storage for your deployment, see the Storage chapter of the *Administration Guide*.

- Prepared storage for additional storage domains, as necessary for the size and design of your environment.

IMPORTANT

If you are using iSCSI storage, the self-hosted engine storage domain must use its own iSCSI target. Any additional storage domains must use a different iSCSI target.

WARNING

Creating additional data storage domains in the same data center as the self-hosted engine storage domain is highly recommended. If you deploy the self-hosted engine in a data center with only one active data storage domain, and that storage domain is corrupted, you will not be able to add new storage domains or remove the corrupted storage domain; you will have to redeploy the self-hosted engine.

Procedure

1. Log in to Cockpit at **https://*HostIPorFQDN*:9090** and click **Virtualization → Hosted Engine**.
2. Click **Start** under the **Hosted Engine** option.
3. Enter the details for the Manager virtual machine:
    a. Enter the **Engine VM FQDN**. This is the FQDN for the Manager virtual machine, not the base host.
    b. Enter a **MAC Address** for the Manager virtual machine, or accept a randomly generated one.
    c. Choose either **DHCP** or **Static** from the **Network Configuration** drop-down list.
        - If you choose **DHCP**, you must have a DHCP reservation for the Manager virtual machine so that its host name resolves to the address received from DHCP. Specify its MAC address in the **MAC Address** field.
        - If you choose **Static**, enter the following details:
            - **VM IP Address** - The IP address must belong to the same subnet as the host. For example, if the host is in 10.1.1.0/24, the Manager virtual machine's IP must be in the same subnet range (10.1.1.1-254/24).
            - **Gateway Address**
            - **DNS Servers**
    d. Select the **Bridge Interface** from the drop-down list.
    e. Enter and confirm the virtual machine's **Root Password**.
    f. Specify whether to allow **Root SSH Access**.
    g. Enter the **Number of Virtual CPUs** for the virtual machine.

   h. Enter the **Memory Size (MiB)**. The available memory is displayed next to the input field.

4. Optionally expand the **Advanced** fields:

   a. Enter a **Root SSH Public Key** to use for root access to the Manager virtual machine.

   b. Select or clear the **Edit Hosts File** check box to specify whether to add entries for the Manager virtual machine and the base host to the virtual machine's **/etc/hosts** file. You must ensure that the host names are resolvable.

   c. Change the management **Bridge Name**, or accept the default **ovirtmgmt**.

   d. Enter the **Gateway Address** for the management bridge.

   e. Enter the **Host FQDN** of the first host to add to the Manager. This is the FQDN of the base host you are running the deployment on.

5. Click **Next**.

6. Enter and confirm the **Admin Portal Password** for the **admin@internal** user.

7. Configure event notifications:

   a. Enter the **Server Name** and **Server Port Number** of the SMTP server.

   b. Enter the **Sender E-Mail Address**.

   c. Enter the **Recipient E-Mail Addresses**.

8. Click **Next**.

9. Review the configuration of the Manager and its virtual machine. If the details are correct, click **Prepare VM**.

10. When the virtual machine installation is complete, click **Next**.

11. Select the **Storage Type** from the drop-down list, and enter the details for the self-hosted engine storage domain:

    - For NFS:

      a. Enter the full address and path to the storage in the **Storage Connection** field.

      b. If required, enter any **Mount Options**.

      c. Enter the **Disk Size (GiB)**.

      d. Select the **NFS Version** from the drop-down list.

      e. Enter the **Storage Domain Name**.

    - For iSCSI:

      a. Enter the **Portal IP Address**, **Portal Port**, **Portal Username**, and **Portal Password**.

      b. Click **Retrieve Target List** and select a target. You can only select one iSCSI target during the deployment, but multipathing is supported to connect all portals of the same portal group.

> **NOTE**
>
> To specify more than one iSCSI target, you must enable multipathing before deploying the self-hosted engine. See *Red Hat Enterprise Linux DM Multipath* for details. There is also a Multipath Helper tool that generates a script to install and configure multipath with different options.

c. Enter the **Disk Size (GiB)**.

d. Enter the **Discovery Username** and **Discovery Password**.

- For Fibre Channel:

  a. Enter the **LUN ID**. The host bus adapters must be configured and connected, and the LUN must not contain any existing data. To reuse an existing LUN, see Reusing LUNs in the *Administration Guide*.

  b. Enter the **Disk Size (GiB)**.

- For Red Hat Gluster Storage:

  a. Enter the full address and path to the storage in the **Storage Connection** field.

  b. If required, enter any **Mount Options**.

  c. Enter the **Disk Size (GiB)**.

12. Click **Next**.

13. Review the storage configuration. If the details are correct, click **Finish Deployment**.

14. When the deployment is complete, click **Close**.
    One data center, cluster, host, storage domain, and the Manager virtual machine are already running. You can log in to the Administration Portal to add any other resources.

15. Enable the required repositories on the Manager virtual machine. See Enabling the Red Hat Virtualization Manager Repositories in the *Installation Guide*.

16. Optionally, add a directory server using the **ovirt-engine-extension-aaa-ldap-setup** interactive setup script so you can add additional users to the environment. For more information, see Configuring an External LDAP Provider in the *Administration Guide*.

The self-hosted engine’s status is displayed in Cockpit’s **Virtualization** → **Hosted Engine** tab. The Manager virtual machine, the host running it, and the self-hosted engine storage domain are flagged with a gold crown in the Administration Portal.

2.2. DEPLOYING THE SELF-HOSTED ENGINE USING THE COMMAND LINE

You can deploy a self-hosted engine from the command line using **hosted-engine --deploy** to collect the details of your environment.

> NOTE
>
> If necessary, you can still use the non-Ansible script from previous versions of Red Hat Virtualization by running **hosted-engine --deploy --noansible**.

Prerequisites

- A fresh installation of Red Hat Virtualization Host or Red Hat Enterprise Linux 7, with the required repositories enabled. See Installing Red Hat Virtualization Host or Enabling the Red Hat Enterprise Linux Host Repositories in the *Installation Guide*.

- A fully qualified domain name prepared for your Manager and the host. Forward and reverse lookup records must both be set in the DNS.

- A directory of at least 5 GB on the host, for the RHV-M Appliance. The deployment process will check if **/var/tmp** has enough space to extract the appliance files. If not, you can specify a different directory or mount external storage. The VDSM user and KVM group must have read, write, and execute permissions on the directory.

- Prepared storage for a data storage domain dedicated to the Manager virtual machine. This storage domain is created during the self-hosted engine deployment, and must be at least 74 GiB. Highly available storage is recommended. For more information on preparing storage for your deployment, see the Storage chapter of the *Administration Guide*.

- Prepared storage for additional storage domains, as necessary for the size and design of your environment.

  > IMPORTANT
  >
  > If you are using iSCSI storage, the self-hosted engine storage domain must use its own iSCSI target. Any additional storage domains must use a different iSCSI target.

  > WARNING
  >
  > Creating additional data storage domains in the same data center as the self-hosted engine storage domain is highly recommended. If you deploy the self-hosted engine in a data center with only one active data storage domain, and that storage domain is corrupted, you will not be able to add new storage domains or remove the corrupted storage domain; you will have to redeploy the self-hosted engine.

Procedure

1. Install the deployment tool:

   ```
   # yum install ovirt-hosted-engine-setup
   ```

2. Red Hat recommends using the **screen** window manager to run the script to avoid losing the session in case of network or terminal disruption. Install and start **screen**:

```
# yum install screen
# screen
```

3. Start the deployment script:

   ```
   # hosted-engine --deploy
   ```

   > NOTE
   >
   > To escape the script at any time, use the **Ctrl**+**D** keyboard combination to abort deployment. In the event of session timeout or connection disruption, run **screen -d -r** to recover the deployment session.

4. Select **Yes** to begin the deployment:

   ```
   Continuing will configure this host for serving as hypervisor and create a local VM with a
   running engine.
   The locally running engine will be used to configure a storage domain and create a VM there.
   At the end the disk of the local VM will be moved to the shared storage.
   Are you sure you want to continue? (Yes, No)[Yes]:
   ```

5. Configure the network. The script detects possible NICs to use as a management bridge for the environment.

   ```
   Please indicate a pingable gateway IP address [X.X.X.X]:
   Please indicate a nic to set ovirtmgmt bridge on: (eth1, eth0) [eth1]:
   ```

6. If you want to use a custom appliance for the virtual machine installation, enter the path to the OVA archive. Otherwise, leave this field empty to use the RHV-M Appliance.

   ```
   If you want to deploy with a custom engine appliance image,
   please specify the path to the OVA archive you would like to use
   (leave it empty to skip, the setup will use rhvm-appliance rpm installing it if missing):
   ```

7. Specify the FQDN for the Manager virtual machine:

   ```
   Please provide the FQDN you would like to use for the engine appliance.
   Note: This will be the FQDN of the engine VM you are now going to launch,
   it should not point to the base host or to any other existing machine.
   Engine VM FQDN:  manager.example.com
   Please provide the domain name you would like to use for the engine appliance.
   Engine VM domain: [example.com]
   ```

8. Enter the root password for the Manager:

   ```
   Enter root password that will be used for the engine appliance:
   Confirm appliance root password:
   ```

9. Enter an SSH public key that will allow you to log in to the Manager as the root user, and specify whether to enable SSH access for the root user:

```
Enter ssh public key for the root user that will be used for the engine appliance (leave it
empty to skip):
Do you want to enable ssh access for the root user (yes, no, without-password) [yes]:
```

10. Enter the virtual machine's CPU and memory configuration:

    ```
    Please specify the number of virtual CPUs for the VM (Defaults to appliance OVF value): [4]:
    Please specify the memory size of the VM in MB (Defaults to maximum available): [7267]:
    ```

11. Enter a MAC address for the Manager virtual machine, or accept a randomly generated one. If you want to provide the Manager virtual machine with an IP address via DHCP, ensure that you have a valid DHCP reservation for this MAC address. The deployment script will not configure the DHCP server for you.

    ```
    You may specify a unicast MAC address for the VM or accept a randomly generated default
    [00:16:3e:3d:34:47]:
    ```

12. Enter the virtual machine's networking details:

    ```
    How should the engine VM network be configured (DHCP, Static)[DHCP]?
    ```

    If you specified **Static**, enter the IP address of the Manager:

    ### IMPORTANT

    The static IP address must belong to the same subnet as the host. For example, if the host is in 10.1.1.0/24, the Manager virtual machine's IP must be in the same subnet range (10.1.1.1-254/24).

    ```
    Please enter the IP address to be used for the engine VM [x.x.x.x]:
    Please provide a comma-separated list (max 3) of IP addresses of domain name servers for
    the engine VM
    Engine VM DNS (leave it empty to skip):
    ```

13. Specify whether to add entries for the Manager virtual machine and the base host to the virtual machine's **/etc/hosts** file. You must ensure that the host names are resolvable.

    ```
    Add lines for the appliance itself and for this host to /etc/hosts on the engine VM?
    Note: ensuring that this host could resolve the engine VM hostname is still up to you (Yes,
    No)[No]
    ```

14. Provide the name and TCP port number of the SMTP server, the email address used to send email notifications, and a comma-separated list of email addresses to receive these notifications:

    ```
    Please provide the name of the SMTP server through which we will send notifications
    [localhost]:
    Please provide the TCP port number of the SMTP server [25]:
    Please provide the email address from which notifications will be sent [root@localhost]:
    Please provide a comma-separated list of email addresses which will get notifications
    [root@localhost]:
    ```

15. Enter a password for the **admin@internal** user to access the Administration Portal:

    ```
    Enter engine admin password:
    Confirm engine admin password:
    ```

    The script creates the virtual machine. This can take some time if it needs to install the RHV-M Appliance.

16. Select the type of storage to use:

    ```
    Please specify the storage you would like to use (glusterfs, iscsi, fc, nfs)[nfs]:
    ```

    - For NFS, enter the version, full address and path to the storage, and any mount options:

      ```
      Please specify the nfs version you would like to use (auto, v3, v4, v4_1)[auto]:
      Please specify the full shared storage connection path to use (example: host:/path):
      storage.example.com:/hosted_engine/nfs
      If needed, specify additional mount options for the connection to the hosted-engine
      storage domain []:
      ```

    - For iSCSI, enter the portal details and select a target and LUN from the auto-detected lists. You can only select one iSCSI target during the deployment, but multipathing is supported to connect all portals of the same portal group.

      NOTE

      To specify more than one iSCSI target, you must enable multipathing before deploying the self-hosted engine. See *Red Hat Enterprise Linux DM Multipath* for details. There is also a Multipath Helper tool that generates a script to install and configure multipath with different options.

      ```
      Please specify the iSCSI portal IP address:
      Please specify the iSCSI portal port [3260]:
      Please specify the iSCSI discover user:
      Please specify the iSCSI discover password:
      Please specify the iSCSI portal login user:
      Please specify the iSCSI portal login password:

      The following targets have been found:
       [1] iqn.2017-10.com.redhat.example:he
        TPGT: 1, portals:
         192.168.1.xxx:3260
         192.168.2.xxx:3260
         192.168.3.xxx:3260

      Please select a target (1) [1]: 1

      The following luns have been found on the requested target:
        [1] 360003ff44dc75adcb5046390a16b4beb   199GiB  MSFT   Virtual HD
            status: free, paths: 1 active

      Please select the destination LUN (1) [1]:
      ```

    - For Gluster storage, enter the full address and path to the storage, and any mount options:

> **IMPORTANT**
>
> Only replica 3 Gluster storage is supported. Ensure you have the following configuration:
>
> - In the **/etc/glusterfs/glusterd.vol** file on all three Gluster servers, set **rpc-auth-allow-insecure** to **on**.
>
>   ```
>   option rpc-auth-allow-insecure on
>   ```
>
> - Configure the volume as follows:
>
>   ```
>   gluster volume set _volume_ cluster.quorum-type auto
>   gluster volume set _volume_ network.ping-timeout 10
>   gluster volume set _volume_ auth.allow \*
>   gluster volume set _volume_ group virt
>   gluster volume set _volume_ storage.owner-uid 36
>   gluster volume set _volume_ storage.owner-gid 36
>   gluster volume set _volume_ server.allow-insecure on
>   ```

```
Please specify the full shared storage connection path to use (example: host:/path):
storage.example.com:/hosted_engine/gluster_volume
If needed, specify additional mount options for the connection to the hosted-engine
storage domain []:
```

- For Fibre Channel, select a LUN from the auto-detected list. The host bus adapters must be configured and connected, and the LUN must not contain any existing data. To reuse an existing LUN, see Reusing LUNs in the *Administration Guide*.

```
The following luns have been found on the requested target:
[1] 3514f0c5447600351   30GiB   XtremIO XtremApp
  status: used, paths: 2 active

[2] 3514f0c5447600352   30GiB   XtremIO XtremApp
  status: used, paths: 2 active

Please select the destination LUN (1, 2) [1]:
```

17. Enter the Manager disk size:

    ```
    Please specify the size of the VM disk in GB: [50]:
    ```

    When the deployment completes successfully, one data center, cluster, host, storage domain, and the Manager virtual machine are already running. You can log in to the Administration Portal to add any other resources.

18. Enable the required repositories on the Manager virtual machine. See Enabling the Red Hat Virtualization Manager Repositories in the *Installation Guide*.

19. Optionally, add a directory server using the **ovirt-engine-extension-aaa-ldap-setup** interactive setup script so you can add additional users to the environment. For more information, see Configuring an External LDAP Provider in the *Administration Guide*.

The Manager virtual machine, the host running it, and the self-hosted engine storage domain are flagged with a gold crown in the Administration Portal.

CHAPTER 3. TROUBLESHOOTING A SELF-HOSTED ENGINE DEPLOYMENT

To confirm whether the self-hosted engine has already been deployed run **hosted-engine --check-deployed**. An error will only be displayed if the self-hosted engine has not been deployed.

3.1. TROUBLESHOOTING THE MANAGER VIRTUAL MACHINE

Check the status of the Manager virtual machine by running **hosted-engine --vm-status**.

> **NOTE**
>
> Any changes made to the Manager virtual machine will take about 20 seconds before they are reflected in the status command output.

Depending on the **Engine status** in the output, see the following suggestions to find or fix the issue.

Engine status: "health": "good", "vm": "up" "detail": "up"

1. If the Manager virtual machine is up and running as normal, you will see the following output:

```
--== Host 1 status ==--

Status up-to-date                  : True
Hostname                           : hypervisor.example.com
Host ID                            : 1
Engine status                      : {"health": "good", "vm": "up", "detail": "up"}
Score                              : 3400
stopped                            : False
Local maintenance                  : False
crc32                              : 99e57eba
Host timestamp                     : 248542
```

2. If the output is normal but you cannot connect to the Manager, check the network connection.

Engine status: "reason": "failed liveliness check", "health": "bad", "vm": "up", "detail": "up"

1. If the **health** is **bad** and the **vm** is **up**, the HA services will try to restart the Manager virtual machine to get the Manager back. If it does not succeed within a few minutes, enable the global maintenance mode from the command line so that the hosts are no longer managed by the HA services.

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

2. Connect to the console. When prompted, enter the operating system's root password. For more console options, see https://access.redhat.com/solutions/2221461.

```
# hosted-engine --console
```

3. Ensure that the Manager virtual machine's operating system is running by logging in.

4. Check the status of the **ovirt-engine** service:

```
# systemctl status -l ovirt-engine
# journalctl -u ovirt-engine
```

5. Check the following logs: **/var/log/messages**, **/var/log/ovirt-engine/engine.log,** and **/var/log/ovirt-engine/server.log**.

6. After fixing the issue, reboot the Manager virtual machine manually from one of the self-hosted engine nodes:

```
# hosted-engine --vm-shutdown
# hosted-engine --vm-start
```

> **NOTE**
>
> When the self-hosted engine nodes are in global maintenance mode, the Manager virtual machine must be rebooted manually. If you try to reboot the Manager virtual machine by sending a **reboot** command from the command line, the Manager virtual machine will remain powered off. This is by design.

7. On the Manager virtual machine, verify that the **ovirt-engine** service is up and running:

```
 # systemctl status ovirt-engine.service
```

8. After ensuring the Manager virtual machine is up and running, close the console session and disable the maintenance mode to enable the HA services again:

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

Engine status: "vm": "down", "health": "bad", "detail": "unknown", "reason": "vm not running on this host"

1. If you have more than one host in your environment, ensure that another host is not currently trying to restart the Manager virtual machine.

2. Ensure that you are not in global maintenance mode.

3. Check the **ovirt-ha-agent** logs in **/var/log/ovirt-hosted-engine-ha/agent.log**.

4. Try to reboot the Manager virtual machine manually from one of the self-hosted engine nodes:

```
# hosted-engine --vm-shutdown
# hosted-engine --vm-start
```

Engine status: "vm": "unknown", "health": "unknown", "detail": "unknown", "reason": "failed to getVmStats"

This status means that **ovirt-ha-agent** failed to get the virtual machine’s details from VDSM.

1. Check the VDSM logs in **/var/log/vdsm/vdsm.log**.

2. Check the **ovirt-ha-agent** logs in **/var/log/ovirt-hosted-engine-ha/agent.log**.

Engine status: The self-hosted engine’s configuration has not been retrieved from shared storage

If you receive the status **The hosted engine configuration has not been retrieved from shared storage. Please ensure that ovirt-ha-agent is running and the storage server is reachable** there is an issue with the **ovirt-ha-agent** service, or with the storage, or both.

1. Check the status of **ovirt-ha-agent** on the host:

   ```
   # systemctl status -l ovirt-ha-agent
   # journalctl -u ovirt-ha-agent
   ```

2. If the **ovirt-ha-agent** is down, restart it:

   ```
   # systemctl start ovirt-ha-agent
   ```

3. Check the **ovirt-ha-agent** logs in **/var/log/ovirt-hosted-engine-ha/agent.log**.

4. Check that you can ping the shared storage.

5. Check whether the shared storage is mounted.

Additional Troubleshooting Commands

> IMPORTANT
>
> Contact the Red Hat Support Team if you feel you need to run any of these commands to troubleshoot your self-hosted engine environment.

- **hosted-engine --reinitialize-lockspace**: This command is used when the sanlock lockspace is broken. Ensure that the global maintenance mode is enabled and that the Manager virtual machine is stopped before reinitializing the sanlock lockspaces.

- **hosted-engine --clean-metadata**: Remove the metadata for a host’s agent from the global status database. This makes all other hosts forget about this host. Ensure that the target host is down and that the global maintenance mode is enabled.

- **hosted-engine --check-liveliness**: This command checks the liveliness page of the ovirt-engine service. You can also check by connecting to **https://*engine-fqdn*/ovirt-engine/services/health/** in a web browser.

- **hosted-engine --connect-storage**: This command instructs VDSM to prepare all storage connections needed for the host and and the Manager virtual machine. This is normally run in the back-end during the self-hosted engine deployment. Ensure that the global maintenance mode is enabled if you need to run this command to troubleshoot storage issues.

3.2. CLEANING UP A FAILED SELF-HOSTED ENGINE DEPLOYMENT

If a self-hosted engine deployment was interrupted, subsequent deployments will fail with an error message. The error will differ depending on the stage in which the deployment failed. If you receive an error message, run the cleanup script to clean up the failed deployment.

Running the Cleanup Script

1. Run **/usr/sbin/ovirt-hosted-engine-cleanup** and select **y** to remove anything left over from the failed self-hosted engine deployment.

```
# /usr/sbin/ovirt-hosted-engine-cleanup
This will de-configure the host to run ovirt-hosted-engine-setup from scratch.
Caution, this operation should be used with care.
Are you sure you want to proceed? [y/n]
```

2. Define whether to reinstall on the same shared storage device or select a different shared storage device.

    - To deploy the installation on the same storage domain, clean up the storage domain by running the following command in the appropriate directory on the server for NFS, Gluster, PosixFS or local storage domains:

        ```
        # rm -rf storage_location/*
        ```

    - For iSCSI or Fibre Channel Protocol (FCP) storage, see https://access.redhat.com/solutions/2121581 for information on how to clean up the storage.

    - Alternatively, select a different shared storage device.

3. Redeploy the self-hosted engine.

CHAPTER 4. ADMINISTERING THE SELF-HOSTED ENGINE

4.1. MAINTAINING THE SELF-HOSTED ENGINE

The maintenance modes enable you to start, stop, and modify the Manager virtual machine without interference from the high-availability agents, and to restart and modify the self-hosted engine nodes in the environment without interfering with the Manager.

There are three maintenance modes that can be enforced:

- **global** - All high-availability agents in the cluster are disabled from monitoring the state of the Manager virtual machine. The global maintenance mode must be applied for any setup or upgrade operations that require the **ovirt-engine** service to be stopped, such as upgrading to a later version of Red Hat Virtualization.
- **local** - The high-availability agent on the node issuing the command is disabled from monitoring the state of the Manager virtual machine. The node is exempt from hosting the Manager virtual machine while in local maintenance mode; if hosting the Manager virtual machine when placed into this mode, the Manager will migrate to another node, provided there is one available. The local maintenance mode is recommended when applying system changes or updates to a self-hosted engine node.
- **none** - Disables maintenance mode, ensuring that the high-availability agents are operating.

Maintaining a RHEL-Based Self-Hosted Engine (Local Maintenance)

1. Place a self-hosted engine node into the local maintenance mode:
    - In the Administration Portal, click **Compute → Hosts** and select a self-hosted engine node.
    - Click **Management → Maintenance**. The local maintenance mode is automatically triggered for that node.
    - You can also set the maintenance mode from the command line:

    ```
    # hosted-engine --set-maintenance --mode=local
    ```
2. After you have completed any maintenance tasks, disable the maintenance mode:

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

Maintaining a RHEL-Based Self-Hosted Engine (Global Maintenance)

1. Place self-hosted engine nodes into global maintenance mode:
    - In the Administration Portal, click **Compute → Hosts**, select any self-hosted engine node, and click **More Actions → Enable Global HA Maintenance**.
    - You can also set the maintenance mode from the command line:

    ```
    # hosted-engine --set-maintenance --mode=global
    ```
2. After you have completed any maintenance tasks, disable the maintenance mode:

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

4.2. ADMINISTERING THE MANAGER VIRTUAL MACHINE

The **hosted-engine** utility is provided to assist with administering the Manager virtual machine. It can be run on any self-hosted engine nodes in the environment. For all the options, run **hosted-engine --help**. For additional information on a specific command, run **hosted-engine --*command* --help**. See Section 3.1, "Troubleshooting the Manager Virtual Machine" for more information.

The following procedure shows you how to update the self-hosted engine configuration file (**/var/lib/ovirt-hosted-engine-ha/broker.conf**) on the shared storage domain after the initial deployment. Currently, you can configure email notifications using SMTP for any HA state transitions on the self-hosted engine nodes. The keys that can be updated include: **smtp-server**, **smtp-port**, **source-email**, **destination-emails**, and **state_transition**.

Updating the Self-Hosted Engine Configuration on the Shared Storage Domain

1. On a self-hosted engine node, set the **smtp-server** key to the desired SMTP server address:

   ```
   # hosted-engine --set-shared-config smtp-server smtp.example.com --type=broker
   ```

   NOTE

   To verify that the self-hosted engine configuration file has been updated, run:

   ```
   # hosted-engine --get-shared-config smtp-server --type=broker
   broker : smtp.example.com, type : broker
   ```

2. Check that the default SMTP port (port 25) has been configured:

   ```
   # hosted-engine --get-shared-config smtp-port --type=broker
   broker : 25, type : broker
   ```

3. Specify an email address you want the SMTP server to use to send out email notifications. Only one address can be specified.

   ```
   # hosted-engine --set-shared-config source-email source@example.com --type=broker
   ```

4. Specify the destination email address to receive email notifications. To specify multiple email addresses, separate each address by a comma.

   ```
   # hosted-engine --set-shared-config destination-emails
   destination1@example.com,destination2@example.com --type=broker
   ```

To verify that SMTP has been properly configured for your self-hosted engine environment, change the HA state on a self-hosted engine node and check if email notifications were sent. For example, you can change the HA state by placing HA agents into maintenance mode. See Section 4.1, "Maintaining the Self-Hosted Engine" for more information.

4.3. CONFIGURING MEMORY SLOTS RESERVED FOR THE SELF-HOSTED ENGINE ON ADDITIONAL HOSTS

If the Manager virtual machine shuts down or needs to be migrated, there must be enough memory on a self-hosted engine node for the Manager virtual machine to restart on or migrate to it. This memory can be reserved on multiple self-hosted engine nodes by using a scheduling policy. The scheduling policy checks if enough memory to start the Manager virtual machine will remain on the specified number of additional self-hosted engine nodes before starting or migrating any virtual machines. See Creating a Scheduling Policy in the *Administration Guide* for more information about scheduling policies.

To add more self-hosted engine nodes to the Red Hat Virtualization Manager, see Section 4.4, “Installing Additional Self-Hosted Engine Nodes”.

Configuring Memory Slots Reserved for the Self-Hosted Engine on Additional Hosts

1. Click **Compute → Clusters** and select the cluster containing the self-hosted engine nodes.

2. Click **Edit**.

3. Click the **Scheduling Policy** tab.

4. Click **+** and select **HeSparesCount**.

5. Enter the number of additional self-hosted engine nodes that will reserve enough free memory to start the Manager virtual machine.

6. Click **OK**.

4.4. INSTALLING ADDITIONAL SELF-HOSTED ENGINE NODES

Additional self-hosted engine nodes are added in the same way as a regular host, with an additional step to deploy the host as a self-hosted engine node. The shared storage domain is automatically detected and the node can be used as a failover host to host the Manager virtual machine when required. You can also attach regular hosts to a self-hosted engine environment, but they cannot host the Manager virtual machine. Red Hat highly recommends having at least two self-hosted engine nodes to ensure the Manager virtual machine is highly available. Additional hosts can also be added using the REST API. See Hosts in the *REST API Guide*.

Prerequisites

- For a RHEL-based self-hosted engine environment, you must have prepared a freshly installed Red Hat Enterprise Linux system on a physical host, and attached the required subscriptions. See Enabling the Red Hat Enterprise Linux Host Repositories in the *Installation Guide* for more information on subscriptions.

- For a RHVH-based self-hosted engine environment, you must have prepared a freshly installed Red Hat Virtualization Host system on a physical host. See Red Hat Virtualization Hosts in the *Installation Guide*.

- If you are reusing a self-hosted engine node, remove its existing self-hosted engine configuration. See Removing a Host from a Self-Hosted Engine Environment .

Procedure

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

2. Click **New**.
   For information on additional host settings, see Explanation of Settings and Controls in the New Host and Edit Host Windows in the *Administration Guide*.

3. Use the drop-down list to select the **Data Center** and **Host Cluster** for the new host.

4. Enter the **Name** and the **Address** of the new host. The standard SSH port, port 22, is auto-filled in the **SSH Port** field.

5. Select an authentication method to use for the Manager to access the host.

   - Enter the root user's password to use password authentication.

   - Alternatively, copy the key displayed in the **SSH PublicKey** field to **/root/.ssh/authorized_keys** on the host to use public key authentication.

6. Optionally, configure power management, where the host has a supported power management card. For information on power management configuration, see Host Power Management Settings Explained in the *Administration Guide*.

7. Click the **Hosted Engine** tab.

8. Select **Deploy**.

9. Click **OK**.

4.5. REINSTALLING AN EXISTING HOST AS A SELF-HOSTED ENGINE NODE

You can convert an existing, regular host in a self-hosted engine environment to a self-hosted engine node capable of hosting the Manager virtual machine.

Procedure

1. Click **Compute → Hosts** and select the host.

2. Click **Management → Maintenance** and click **OK**.

3. Click **Installation → Reinstall**.

4. Click the **Hosted Engine** tab and select **DEPLOY** from the drop-down list.

5. Click **OK**.

The host is reinstalled with self-hosted engine configuration, and is flagged with a crown icon in the Administration Portal.

4.6. REMOVING A HOST FROM A SELF-HOSTED ENGINE ENVIRONMENT

To remove a self-hosted engine node from your environment, place the node into maintenance mode, undeploy the node, and optionally remove it. The node can be managed as a regular host after the HA services have been stopped, and the self-hosted engine configuration files have been removed.

Removing a Host from a Self-Hosted Engine Environment

1. In the Administration Portal, click **Compute → Hosts** and select the self-hosted engine node.

2. Click **Management → Maintenance** and click **OK**.

3. Click **Installation** → **Reinstall**.

4. Click the **Hosted Engine** tab and select **UNDEPLOY** from the drop-down list. This action stops the **ovirt-ha-agent** and **ovirt-ha-broker** services and removes the self-hosted engine configuration file.

5. Click **OK**.

6. Optionally, click **Remove** to open the **Remove Host(s)** confirmation window and click **OK**.

4.7. UPDATING THE MANAGER VIRTUAL MACHINE

To update a self-hosted engine from your current version of 4.2 to the latest version of 4.2, you must place the environment in global maintenance mode and then follow the standard procedure for updating between minor versions.

Enabling Global Maintenance Mode

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

Procedure

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

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

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

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

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.

Disabling Global Maintenance Mode

Procedure

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

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

2. Confirm that the environment is running:

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

CHAPTER 5. MIGRATING FROM A STANDALONE MANAGER TO A SELF-HOSTED ENGINE

You can convert a standalone Red Hat Virtualization Manager (a separate physical machine, or a virtual machine hosted in a separate virtualization environment) to a self-hosted engine by backing up the standalone Manager and restoring it in a new self-hosted environment.

When you specify a backup file during self-hosted engine deployment, the Manager backup is restored on a new virtual machine, with a dedicated self-hosted engine storage domain. Deploying on a fresh host is highly recommended; if the host used for deployment existed in the backed up environment, it will be removed from the restored database to avoid conflicts in the new environment.

At least two self-hosted engine nodes are required for the Manager virtual machine to be highly available. You can add new nodes, or convert existing hosts.

The migration involves the following key actions:

1. Back up the original Manager using the **engine-backup** tool.
2. Deploy a new self-hosted engine and restore the backup.
3. Enable the Manager repositories on the new Manager virtual machine.
4. Convert regular hosts to self-hosted engine nodes that can host the new Manager.

This procedure assumes that you have access and can make changes to the original Manager.

Prerequisites

- A fresh installation of Red Hat Virtualization Host or Red Hat Enterprise Linux 7, with the required repositories enabled. See Installing Red Hat Virtualization Host or Enabling the Red Hat Enterprise Linux Host Repositories in the *Installation Guide*.
- A fully qualified domain name prepared for your Manager and the host. Forward and reverse lookup records must both be set in the DNS. The new Manager must have the same fully qualified domain name as the original Manager.
- A directory of at least 5 GB on the host, for the RHV-M Appliance. The deployment process will check if **/var/tmp** has enough space to extract the appliance files. If not, you can specify a different directory or mount external storage. The VDSM user and KVM group must have read, write, and execute permissions on the directory.
- Prepared storage for a data storage domain dedicated to the Manager virtual machine. This storage domain is created during the self-hosted engine deployment, and must be at least 74 GiB. Highly available storage is recommended. For more information on preparing storage for your deployment, see the Storage chapter of the *Administration Guide*.

IMPORTANT

If you are using iSCSI storage, the self-hosted engine storage domain must use its own iSCSI target. Any additional storage domains must use a different iSCSI target.

> **WARNING**
>
> Creating additional data storage domains in the same data center as the self-hosted engine storage domain is highly recommended. If you deploy the self-hosted engine in a data center with only one active data storage domain, and that storage domain is corrupted, you will not be able to add new storage domains or remove the corrupted storage domain; you will have to redeploy the self-hosted engine.

- The management network (**ovirtmgmt** by default) must be configured as a **VM network**, so that it can manage the Manager virtual machine.
- The original Manager must be updated to the latest minor version; the Manager version in the backup file must match the version of the new Manager. See Updating the Red Hat Virtualization Manager in the *Upgrade Guide*.

5.1. BACKING UP THE ORIGINAL MANAGER

Back up the original Manager using the **engine-backup** command, and copy the backup file to a separate location so that it can be accessed at any point during the process.

For more information about **engine-backup --mode=backup** options, see Backing Up and Restoring the Red Hat Virtualization Manager in the *Administration Guide*.

Procedure

1. Log in to the original Manager and stop the **ovirt-engine** service:

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

> **NOTE**
>
> Though stopping the original Manager from running is not obligatory, it is recommended as it ensures no changes are made to the environment after the backup is created. Additionally, it prevents the original Manager and the new Manager from simultaneously managing existing resources.

2. Run the **engine-backup** command, specifying the name of the backup file to create, and the name of the log file to create to store the backup log:

```
# engine-backup --mode=backup --file=file_name --log=log_file_name
```

3. Copy the files to an external server. In the following example, **storage.example.com** is the fully qualified domain name of a network storage server that will store the backup until it is needed, and /**backup**/ is any designated folder or path.

```
# scp -p file_name log_file_name storage.example.com:/backup/
```

4. If you do not require the Manager machine for other purposes, unregister it from Red Hat Subscription Manager:

   ```
   # subscription-manager unregister
   ```

After backing up the Manager, deploy a new self-hosted engine and restore the backup on the new virtual machine.

5.2. RESTORING THE BACKUP ON A NEW SELF-HOSTED ENGINE

Run the **hosted-engine** script on a new host, and use the **--restore-from-file=*path/to/file_name*** option to restore the Manager backup during the deployment.

> IMPORTANT
>
> If you are using iSCSI storage, and your iSCSI target filters connections according to the initiator's ACL, the deployment may fail with a **STORAGE_DOMAIN_UNREACHABLE** error. To prevent this, you must update your iSCSI configuration before beginning the self-hosted engine deployment:
>
> - If you are redeploying on an existing host, you must update the host's iSCSI initiator settings in **/etc/iscsi/initiatorname.iscsi**. The initiator IQN must be the same as was previously mapped on the iSCSI target, or updated to a new IQN, if applicable.
> - If you are deploying on a fresh host, you must update the iSCSI target configuration to accept connections from that host.
>
> Note that the IQN can be updated on the host side (iSCSI initiator), or on the storage side (iSCSI target).

Procedure

1. Copy the backup file to the new host. In the following example, **host.example.com** is the FQDN for the host, and /**backup**/ is any designated folder or path.

   ```
   # scp -p file_name host.example.com:/backup/
   ```

2. Log in to the new host. If you are deploying on Red Hat Virtualization Host, the self-hosted engine deployment tool is available by default. If you are deploying on Red Hat Enterprise Linux, you must install the package:

   ```
   # yum install ovirt-hosted-engine-setup
   ```

3. Red Hat recommends using the **screen** window manager to run the script to avoid losing the session in case of network or terminal disruption. Install and run **screen**:

   ```
   # yum install screen
   # screen
   ```

   In the event of session timeout or connection disruption, run **screen -d -r** to recover the deployment session.

4. Run the **hosted-engine** script, specifying the path to the backup file:

```
# hosted-engine --deploy --restore-from-file=backup/file_name
```

To escape the script at any time, use **CTRL**+**D** to abort deployment.

5. Select **Yes** to begin the deployment.
6. Configure the network. The script detects possible NICs to use as a management bridge for the environment.
7. If you want to use a custom appliance for the virtual machine installation, enter the path to the OVA archive. Otherwise, leave this field empty to use the RHV-M Appliance.
8. Specify the FQDN for the Manager virtual machine.
9. Enter the root password for the Manager.
10. Enter an SSH public key that will allow you to log in to the Manager as the root user, and specify whether to enable SSH access for the root user.
11. Enter the virtual machine's CPU and memory configuration.

    NOTE

    The virtual machine must have the same amount of RAM as the physical machine from which the Manager is being migrated. If you must migrate to a virtual machine that has less RAM than the physical machine from which the Manager is migrated, see https://access.redhat.com/articles/2705841.

12. Enter a MAC address for the Manager virtual machine, or accept a randomly generated one. If you want to provide the Manager virtual machine with an IP address via DHCP, ensure that you have a valid DHCP reservation for this MAC address. The deployment script will not configure the DHCP server for you.
13. Enter the virtual machine's networking details. If you specify **Static**, enter the IP address of the Manager.

    IMPORTANT

    The static IP address must belong to the same subnet as the host. For example, if the host is in 10.1.1.0/24, the Manager virtual machine's IP must be in the same subnet range (10.1.1.1-254/24).

14. Specify whether to add entries for the Manager virtual machine and the base host to the virtual machine's **/etc/hosts** file. You must ensure that the host names are resolvable.
15. Provide the name and TCP port number of the SMTP server, the email address used to send email notifications, and a comma-separated list of email addresses to receive these notifications:
16. Enter a password for the **admin@internal** user to access the Administration Portal.
    The script creates the virtual machine. This can take some time if the RHV-M Appliance needs to be installed.
17. Select the type of storage to use:
    - For NFS, enter the version, full address and path to the storage, and any mount options

- For NFS, enter the version, full address and path to the storage, and any mount options.

- For iSCSI, enter the portal details and select a target and LUN from the auto-detected lists. You can only select one iSCSI target during the deployment, but multipathing is supported to connect all portals of the same portal group.

  NOTE

  To specify more than one iSCSI target, you must enable multipathing before deploying the self-hosted engine. See *Red Hat Enterprise Linux DM Multipath* for details. There is also a Multipath Helper tool that generates a script to install and configure multipath with different options.

- For Gluster storage, enter the full address and path to the storage, and any mount options.

  IMPORTANT

  Only replica 3 Gluster storage is supported. Ensure you have the following configuration:

  - In the **/etc/glusterfs/glusterd.vol** file on all three Gluster servers, set **rpc-auth-allow-insecure** to **on**.

    ```
    option rpc-auth-allow-insecure on
    ```

  - Configure the volume as follows:

    ```
    gluster volume set _volume_ cluster.quorum-type auto
    gluster volume set _volume_ network.ping-timeout 10
    gluster volume set _volume_ auth.allow \*
    gluster volume set _volume_ group virt
    gluster volume set _volume_ storage.owner-uid 36
    gluster volume set _volume_ storage.owner-gid 36
    gluster volume set _volume_ server.allow-insecure on
    ```

- For Fibre Channel, select a LUN from the auto-detected list. The host bus adapters must be configured and connected, and the LUN must not contain any existing data. To reuse an existing LUN, see Reusing LUNs in the *Administration Guide*.

18. Enter the Manager disk size.
    The script continues until the deployment is complete.

19. The deployment process changes the Manager's SSH keys. To allow client machines to access the new Manager without SSH errors, remove the original Manager's entry from the **.ssh/known_hosts** file on any client machines that accessed the original Manager.

When the deployment is complete, log in to the new Manager virtual machine and enable the required repositories.

5.3. ENABLING THE RED HAT VIRTUALIZATION MANAGER REPOSITORIES

Register the system with Red Hat Subscription Manager, attach the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscriptions, and enable the Manager repositories.

Procedure

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

```
# subscription-manager register
```

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

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

3. Use the pool IDs to attach the subscriptions to the system:

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

> **NOTE**
>
> To view currently attached subscriptions:
>
> ```
> # subscription-manager list --consumed
> ```
>
> To list all enabled repositories:
>
> ```
> # yum repolist
> ```

4. Configure the repositories:

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-7-server-rpms \
    --enable=rhel-7-server-supplementary-rpms \
    --enable=rhel-7-server-rhv-4.2-manager-rpms \
    --enable=rhel-7-server-rhv-4-manager-tools-rpms \
    --enable=rhel-7-server-ansible-2.9-rpms \
    --enable=jb-eap-7-for-rhel-7-server-rpms
```

The Red Hat Virtualization Manager has been migrated to a self-hosted engine setup. The Manager is now operating on a virtual machine on the new self-hosted engine node.

The hosts will be running in the new environment, but cannot host the Manager virtual machine. You can convert some or all of these hosts to self-hosted engine nodes.

5.4. REINSTALLING AN EXISTING HOST AS A SELF-HOSTED ENGINE NODE

You can convert an existing, regular host in a self-hosted engine environment to a self-hosted engine node capable of hosting the Manager virtual machine.

Procedure

1. Click **Compute → Hosts** and select the host.

2. Click **Management → Maintenance** and click **OK**.

3. Click **Installation → Reinstall**.

4. Click the **Hosted Engine** tab and select **DEPLOY** from the drop-down list.

5. Click **OK**.

The host is reinstalled with self-hosted engine configuration, and is flagged with a crown icon in the Administration Portal.

After reinstalling the hosts as self-hosted engine nodes, you can check the status of the new environment by running the following command on one of the nodes:

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

If the new environment is running without issue, you can decommission the original physical Manager machine.

CHAPTER 6. BACKING UP AND RESTORING A SELF-HOSTED ENGINE

You can back up a self-hosted engine and restore it in a new self-hosted environment. Use this procedure for tasks such as migrating the environment to a new self-hosted engine storage domain with a different storage type.

When you specify a backup file during deployment, the backup is restored on a new Manager virtual machine, with a new self-hosted engine storage domain. The old Manager is removed, and the old self-hosted engine storage domain is renamed and can be manually removed after you confirm that the new environment is working correctly. Deploying on a fresh host is highly recommended; if the host used for deployment existed in the backed up environment, it will be removed from the restored database to avoid conflicts in the new environment.

The backup and restore operation involves the following key actions:

1. Back up the original Manager using the **engine-backup** tool.
2. Deploy a new self-hosted engine and restore the backup.
3. Enable the Manager repositories on the new Manager virtual machine.
4. Reinstall the self-hosted engine nodes to update their configuration.
5. Remove the old self-hosted engine storage domain.

This procedure assumes that you have access and can make changes to the original Manager.

Prerequisites

- A fresh installation of Red Hat Virtualization Host or Red Hat Enterprise Linux 7, with the required repositories enabled. See Installing Red Hat Virtualization Host or Enabling the Red Hat Enterprise Linux Host Repositories in the *Installation Guide*.
- A fully qualified domain name prepared for your Manager and the host. Forward and reverse lookup records must both be set in the DNS. The new Manager must have the same fully qualified domain name as the original Manager.
- A directory of at least 5 GB on the host, for the RHV-M Appliance. The deployment process will check if **/var/tmp** has enough space to extract the appliance files. If not, you can specify a different directory or mount external storage. The VDSM user and KVM group must have read, write, and execute permissions on the directory.
- Prepared storage for a data storage domain dedicated to the Manager virtual machine. This storage domain is created during the self-hosted engine deployment, and must be at least 74 GiB. Highly available storage is recommended. For more information on preparing storage for your deployment, see the Storage chapter of the *Administration Guide*.

> **WARNING**
>
> If you are using NFS or Gluster storage, do not use the old self-hosted engine storage domain's mount point to deploy the new storage domain, as you risk losing virtual machine data.

> **IMPORTANT**
>
> If you are using iSCSI storage, the self-hosted engine storage domain must use its own iSCSI target. Any additional storage domains must use a different iSCSI target.

- The original Manager must be updated to the latest minor version; the Manager version in the backup file must match the version of the new Manager. See Updating the Red Hat Virtualization Manager in the *Upgrade Guide*.
- There must be at least one regular host in the environment. This host (and any other regular hosts) will remain active to host the SPM role and any running virtual machines. If a regular host is not already the SPM, move the SPM role before creating the backup by selecting a regular host and clicking **Management → Select as SPM**.
  If no regular hosts are available, there are two ways to add one:
  - Remove the self-hosted engine configuration from a node (but do not remove the node from the environment). See Section 4.6, "Removing a Host from a Self-Hosted Engine Environment".
  - Add a new regular host. See Adding a Host to the Red Hat Virtualization Manager in the *Installation Guide*.

6.1. BACKING UP THE ORIGINAL MANAGER

Back up the original Manager using the **engine-backup** command, and copy the backup file to a separate location so that it can be accessed at any point during the process.

For more information about **engine-backup --mode=backup** options, see Backing Up and Restoring the Red Hat Virtualization Manager in the *Administration Guide*.

Procedure

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

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

2. Log in to the original Manager and stop the **ovirt-engine** service:

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

NOTE

Though stopping the original Manager from running is not obligatory, it is recommended as it ensures no changes are made to the environment after the backup is created. Additionally, it prevents the original Manager and the new Manager from simultaneously managing existing resources.

3. Run the **engine-backup** command, specifying the name of the backup file to create, and the name of the log file to create to store the backup log:

```
# engine-backup --mode=backup --file=file_name --log=log_file_name
```

4. Copy the files to an external server. In the following example, **storage.example.com** is the fully qualified domain name of a network storage server that will store the backup until it is needed, and /**backup**/ is any designated folder or path.

```
# scp -p file_name log_file_name storage.example.com:/backup/
```

5. If you do not require the Manager machine for other purposes, unregister it from Red Hat Subscription Manager:

```
# subscription-manager unregister
```

6. Log in to one of the self-hosted engine nodes and shut down the original Manager virtual machine:

```
# hosted-engine --vm-shutdown
```

After backing up the Manager, deploy a new self-hosted engine and restore the backup on the new virtual machine.

6.2. RESTORING THE BACKUP ON A NEW SELF-HOSTED ENGINE

Run the **hosted-engine** script on a new host, and use the **--restore-from-file=*path/to/file_name*** option to restore the Manager backup during the deployment.

IMPORTANT

If you are using iSCSI storage, and your iSCSI target filters connections according to the initiator’s ACL, the deployment may fail with a **STORAGE_DOMAIN_UNREACHABLE** error. To prevent this, you must update your iSCSI configuration before beginning the self-hosted engine deployment:

- If you are redeploying on an existing host, you must update the host’s iSCSI initiator settings in **/etc/iscsi/initiatorname.iscsi**. The initiator IQN must be the same as was previously mapped on the iSCSI target, or updated to a new IQN, if applicable.

- If you are deploying on a fresh host, you must update the iSCSI target configuration to accept connections from that host.

Note that the IQN can be updated on the host side (iSCSI initiator), or on the storage side (iSCSI target).

Procedure

1. Copy the backup file to the new host. In the following example, **host.example.com** is the FQDN for the host, and /**backup**/ is any designated folder or path.

   ```
   # scp -p file_name host.example.com:/backup/
   ```

2. Log in to the new host. If you are deploying on Red Hat Virtualization Host, the self-hosted engine deployment tool is available by default. If you are deploying on Red Hat Enterprise Linux, you must install the package:

   ```
   # yum install ovirt-hosted-engine-setup
   ```

3. Red Hat recommends using the **screen** window manager to run the script to avoid losing the session in case of network or terminal disruption. Install and run **screen**:

   ```
   # yum install screen
   # screen
   ```

   In the event of session timeout or connection disruption, run **screen -d -r** to recover the deployment session.

4. Run the **hosted-engine** script, specifying the path to the backup file:

   ```
   # hosted-engine --deploy --restore-from-file=backup/file_name
   ```

   To escape the script at any time, use **CTRL**+**D** to abort deployment.

5. Select **Yes** to begin the deployment.

6. Configure the network. The script detects possible NICs to use as a management bridge for the environment.

7. If you want to use a custom appliance for the virtual machine installation, enter the path to the OVA archive. Otherwise, leave this field empty to use the RHV-M Appliance.

8. Specify the FQDN for the Manager virtual machine.

9. Enter the root password for the Manager.

10. Enter an SSH public key that will allow you to log in to the Manager as the root user, and specify whether to enable SSH access for the root user.

11. Enter the virtual machine’s CPU and memory configuration.

12. Enter a MAC address for the Manager virtual machine, or accept a randomly generated one. If you want to provide the Manager virtual machine with an IP address via DHCP, ensure that you have a valid DHCP reservation for this MAC address. The deployment script will not configure the DHCP server for you.

13. Enter the virtual machine’s networking details. If you specify **Static**, enter the IP address of the Manager.

IMPORTANT

The static IP address must belong to the same subnet as the host. For example, if the host is in 10.1.1.0/24, the Manager virtual machine's IP must be in the same subnet range (10.1.1.1-254/24).

14. Specify whether to add entries for the Manager virtual machine and the base host to the virtual machine's **/etc/hosts** file. You must ensure that the host names are resolvable.

15. Provide the name and TCP port number of the SMTP server, the email address used to send email notifications, and a comma-separated list of email addresses to receive these notifications:

16. Enter a password for the **admin@internal** user to access the Administration Portal.
    The script creates the virtual machine. This can take some time if the RHV-M Appliance needs to be installed.

17. Select the type of storage to use:

    - For NFS, enter the version, full address and path to the storage, and any mount options.

      WARNING

      Do not use the old self-hosted engine storage domain's mount point for the new storage domain, as you risk losing virtual machine data.

    - For iSCSI, enter the portal details and select a target and LUN from the auto-detected lists. You can only select one iSCSI target during the deployment, but multipathing is supported to connect all portals of the same portal group.

      NOTE

      To specify more than one iSCSI target, you must enable multipathing before deploying the self-hosted engine. See *Red Hat Enterprise Linux DM Multipath* for details. There is also a Multipath Helper tool that generates a script to install and configure multipath with different options.

    - For Gluster storage, enter the full address and path to the storage, and any mount options.

      WARNING

      Do not use the old self-hosted engine storage domain's mount point for the new storage domain, as you risk losing virtual machine data.

IMPORTANT

Only replica 3 Gluster storage is supported. Ensure you have the following configuration:

- In the **/etc/glusterfs/glusterd.vol** file on all three Gluster servers, set **rpc-auth-allow-insecure** to **on**.

  ```
  option rpc-auth-allow-insecure on
  ```

- Configure the volume as follows:

  ```
  gluster volume set _volume_ cluster.quorum-type auto
  gluster volume set _volume_ network.ping-timeout 10
  gluster volume set _volume_ auth.allow \*
  gluster volume set _volume_ group virt
  gluster volume set _volume_ storage.owner-uid 36
  gluster volume set _volume_ storage.owner-gid 36
  gluster volume set _volume_ server.allow-insecure on
  ```

- For Fibre Channel, select a LUN from the auto-detected list. The host bus adapters must be configured and connected, and the LUN must not contain any existing data. To reuse an existing LUN, see Reusing LUNs in the *Administration Guide*.

18. Enter the Manager disk size.
    The script continues until the deployment is complete.

19. The deployment process changes the Manager's SSH keys. To allow client machines to access the new Manager without SSH errors, remove the original Manager's entry from the **.ssh/known_hosts** file on any client machines that accessed the original Manager.

When the deployment is complete, log in to the new Manager virtual machine and enable the required repositories.

6.3. ENABLING THE RED HAT VIRTUALIZATION MANAGER REPOSITORIES

Register the system with Red Hat Subscription Manager, attach the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscriptions, and enable the Manager repositories.

Procedure

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

   ```
   # subscription-manager register
   ```

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

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

3. Use the pool IDs to attach the subscriptions to the system:

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

NOTE

To view currently attached subscriptions:

```
# subscription-manager list --consumed
```

To list all enabled repositories:

```
# yum repolist
```

4. Configure the repositories:

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-7-server-rpms \
    --enable=rhel-7-server-supplementary-rpms \
    --enable=rhel-7-server-rhv-4.2-manager-rpms \
    --enable=rhel-7-server-rhv-4-manager-tools-rpms \
    --enable=rhel-7-server-ansible-2.9-rpms \
    --enable=jb-eap-7-for-rhel-7-server-rpms
```

The Manager and its resources are now running in the new self-hosted environment. The self-hosted engine nodes must be reinstalled in the Manager to update their self-hosted engine configuration. Standard hosts are not affected. Perform the following procedure for each self-hosted engine node.

6.4. REINSTALLING HOSTS

Reinstall Red Hat Virtualization Hosts (RHVH) and Red Hat Enterprise Linux hosts from the Administration Portal. The procedure includes stopping and restarting the host.

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 reinstalls are performed at a time when the host’s usage is relatively low.
- Ensure that the cluster 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 moving the host to maintenance.
- Ensure that the cluster contains more than one host before performing a reinstall. Do not attempt to reinstall all the hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.

Procedure

1. Click **Compute → Hosts** and select the host.
2. Click **Management → Maintenance**.

3. Click **Installation → Reinstall** to open the **Install Host** window.

4. Click the **Hosted Engine** tab and select **DEPLOY** from the drop-down list.

5. Click **OK** to reinstall the host.

Once successfully reinstalled, the host displays a status of **Up**. Any virtual machines that were migrated off the host can now be migrated back to it.

IMPORTANT

After a Red Hat Virtualization Host is successfully registered to the Red Hat Virtualization Manager and then reinstalled, it may erroneously appear in the Administration Portal with the status of **Install Failed**. Click **Management → Activate**, and the host will change to an **Up** status and be ready for use.

After reinstalling the self-hosted engine nodes, you can check the status of the new environment by running the following command on one of the nodes:

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

During the restoration, the old self-hosted engine storage domain was renamed, but was not removed from the new environment in case the restoration was faulty. After confirming that the environment is running normally, you can remove the old self-hosted engine storage domain.

6.5. REMOVING A STORAGE DOMAIN

You have a storage domain in your data center that you want to remove from the virtualized environment.

Procedure

1. Click **Storage → Domains**.

2. Move the storage domain to maintenance mode and detach it:

    a. Click the storage domain's name to open the details view.

    b. Click the **Data Center** tab.

    c. Click **Maintenance**, then click **OK**.

    d. Click **Detach**, then click **OK**.

3. Click **Remove**.

4. Optionally select the **Format Domain, i.e. Storage Content will be lost!**check box to erase the content of the domain.

5. Click **OK**.

The storage domain is permanently removed from the environment.

CHAPTER 7. RECOVERING A SELF-HOSTED ENGINE FROM AN EXISTING BACKUP

If a self-hosted engine is unavailable due to problems that cannot be repaired, you can restore it in a new self-hosted environment using a backup taken before the problem began, if one is available.

When you specify a backup file during deployment, the backup is restored on a new Manager virtual machine, with a new self-hosted engine storage domain. The old Manager is removed, and the old self-hosted engine storage domain is renamed and can be manually removed after you confirm that the new environment is working correctly. Deploying on a fresh host is highly recommended; if the host used for deployment existed in the backed up environment, it will be removed from the restored database to avoid conflicts in the new environment.

Restoring a self-hosted engine involves the following key actions:

1. Deploy a new self-hosted engine and restore the backup.
2. Enable the Manager repositories on the new Manager virtual machine.
3. Reinstall the self-hosted engine nodes to update their configuration.
4. Remove the old self-hosted engine storage domain.

This procedure assumes that you do not have access to the original Manager, and that the new host can access the backup file.

Prerequisites

- A fresh installation of Red Hat Virtualization Host or Red Hat Enterprise Linux 7, with the required repositories enabled. See Installing Red Hat Virtualization Host or Enabling the Red Hat Enterprise Linux Host Repositories in the *Installation Guide*.
- A fully qualified domain name prepared for your Manager and the host. Forward and reverse lookup records must both be set in the DNS. The new Manager must have the same fully qualified domain name as the original Manager.
- A directory of at least 5 GB on the host, for the RHV-M Appliance. The deployment process will check if **/var/tmp** has enough space to extract the appliance files. If not, you can specify a different directory or mount external storage. The VDSM user and KVM group must have read, write, and execute permissions on the directory.
- Prepared storage for a data storage domain dedicated to the Manager virtual machine. This storage domain is created during the self-hosted engine deployment, and must be at least 74 GiB. Highly available storage is recommended. For more information on preparing storage for your deployment, see the Storage chapter of the *Administration Guide*.

> **WARNING**
>
> If you are using NFS or Gluster storage, do not use the old self-hosted engine storage domain’s mount point to deploy the new storage domain, as you risk losing virtual machine data.

IMPORTANT

If you are using iSCSI storage, the self-hosted engine storage domain must use its own iSCSI target. Any additional storage domains must use a different iSCSI target.

7.1. RESTORING THE BACKUP ON A NEW SELF-HOSTED ENGINE

Run the **hosted-engine** script on a new host, and use the **--restore-from-file=*path/to/file_name*** option to restore the Manager backup during the deployment.

IMPORTANT

If you are using iSCSI storage, and your iSCSI target filters connections according to the initiator's ACL, the deployment may fail with a **STORAGE_DOMAIN_UNREACHABLE** error. To prevent this, you must update your iSCSI configuration before beginning the self-hosted engine deployment:

- If you are redeploying on an existing host, you must update the host's iSCSI initiator settings in **/etc/iscsi/initiatorname.iscsi**. The initiator IQN must be the same as was previously mapped on the iSCSI target, or updated to a new IQN, if applicable.
- If you are deploying on a fresh host, you must update the iSCSI target configuration to accept connections from that host.

Note that the IQN can be updated on the host side (iSCSI initiator), or on the storage side (iSCSI target).

Procedure

1. Copy the backup file to the new host. In the following example, **host.example.com** is the FQDN for the host, and /**backup**/ is any designated folder or path.

   ```
   # scp -p file_name host.example.com:/backup/
   ```

2. Log in to the new host. If you are deploying on Red Hat Virtualization Host, the self-hosted engine deployment tool is available by default. If you are deploying on Red Hat Enterprise Linux, you must install the package:

   ```
   # yum install ovirt-hosted-engine-setup
   ```

3. Red Hat recommends using the **screen** window manager to run the script to avoid losing the session in case of network or terminal disruption. Install and run **screen**:

   ```
   # yum install screen
   # screen
   ```

   In the event of session timeout or connection disruption, run **screen -d -r** to recover the deployment session.

4. Run the **hosted-engine** script, specifying the path to the backup file:

   ```
   # hosted-engine --deploy --restore-from-file=backup/file_name
   ```

To escape the script at any time, use **CTRL**+**D** to abort deployment.

5. Select **Yes** to begin the deployment.

6. Configure the network. The script detects possible NICs to use as a management bridge for the environment.

7. If you want to use a custom appliance for the virtual machine installation, enter the path to the OVA archive. Otherwise, leave this field empty to use the RHV-M Appliance.

8. Specify the FQDN for the Manager virtual machine.

9. Enter the root password for the Manager.

10. Enter an SSH public key that will allow you to log in to the Manager as the root user, and specify whether to enable SSH access for the root user.

11. Enter the virtual machine's CPU and memory configuration.

12. Enter a MAC address for the Manager virtual machine, or accept a randomly generated one. If you want to provide the Manager virtual machine with an IP address via DHCP, ensure that you have a valid DHCP reservation for this MAC address. The deployment script will not configure the DHCP server for you.

13. Enter the virtual machine's networking details. If you specify **Static**, enter the IP address of the Manager.

    IMPORTANT

    The static IP address must belong to the same subnet as the host. For example, if the host is in 10.1.1.0/24, the Manager virtual machine's IP must be in the same subnet range (10.1.1.1-254/24).

14. Specify whether to add entries for the Manager virtual machine and the base host to the virtual machine's **/etc/hosts** file. You must ensure that the host names are resolvable.

15. Provide the name and TCP port number of the SMTP server, the email address used to send email notifications, and a comma-separated list of email addresses to receive these notifications:

16. Enter a password for the **admin@internal** user to access the Administration Portal.
    The script creates the virtual machine. This can take some time if the RHV-M Appliance needs to be installed.

17. Select the type of storage to use:

    - For NFS, enter the version, full address and path to the storage, and any mount options.

      WARNING

      Do not use the old self-hosted engine storage domain's mount point for the new storage domain, as you risk losing virtual machine data.

- For iSCSI, enter the portal details and select a target and LUN from the auto-detected lists. You can only select one iSCSI target during the deployment, but multipathing is supported to connect all portals of the same portal group.

  NOTE

  To specify more than one iSCSI target, you must enable multipathing before deploying the self-hosted engine. See *Red Hat Enterprise Linux DM Multipath* for details. There is also a Multipath Helper tool that generates a script to install and configure multipath with different options.

- For Gluster storage, enter the full address and path to the storage, and any mount options.

  WARNING

  Do not use the old self-hosted engine storage domain's mount point for the new storage domain, as you risk losing virtual machine data.

  IMPORTANT

  Only replica 3 Gluster storage is supported. Ensure you have the following configuration:

  - In the **/etc/glusterfs/glusterd.vol** file on all three Gluster servers, set **rpc-auth-allow-insecure** to **on**.

    ```
    option rpc-auth-allow-insecure on
    ```

  - Configure the volume as follows:

    ```
    gluster volume set _volume_ cluster.quorum-type auto
    gluster volume set _volume_ network.ping-timeout 10
    gluster volume set _volume_ auth.allow \*
    gluster volume set _volume_ group virt
    gluster volume set _volume_ storage.owner-uid 36
    gluster volume set _volume_ storage.owner-gid 36
    gluster volume set _volume_ server.allow-insecure on
    ```

- For Fibre Channel, select a LUN from the auto-detected list. The host bus adapters must be configured and connected, and the LUN must not contain any existing data. To reuse an existing LUN, see Reusing LUNs in the *Administration Guide*.

18. Enter the Manager disk size.
    The script continues until the deployment is complete.

19. The deployment process changes the Manager's SSH keys. To allow client machines to access the new Manager without SSH errors, remove the original Manager's entry from the **.ssh/known_hosts** file on any client machines that accessed the original Manager.

When the deployment is complete, log in to the new Manager virtual machine and enable the required repositories.

7.2. ENABLING THE RED HAT VIRTUALIZATION MANAGER REPOSITORIES

Register the system with Red Hat Subscription Manager, attach the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscriptions, and enable the Manager repositories.

Procedure

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

   ```
   # subscription-manager register
   ```

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

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

3. Use the pool IDs to attach the subscriptions to the system:

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

   NOTE

   To view currently attached subscriptions:

   ```
   # subscription-manager list --consumed
   ```

   To list all enabled repositories:

   ```
   # yum repolist
   ```

4. Configure the repositories:

   ```
   # subscription-manager repos \
       --disable='*' \
       --enable=rhel-7-server-rpms \
       --enable=rhel-7-server-supplementary-rpms \
       --enable=rhel-7-server-rhv-4.2-manager-rpms \
       --enable=rhel-7-server-rhv-4-manager-tools-rpms \
       --enable=rhel-7-server-ansible-2.9-rpms \
       --enable=jb-eap-7-for-rhel-7-server-rpms
   ```

The Manager and its resources are now running in the new self-hosted environment. The self-hosted engine nodes must be reinstalled in the Manager to update their self-hosted engine configuration. Standard hosts are not affected. Perform the following procedure for each self-hosted engine node.

7.3. REINSTALLING HOSTS

Reinstall Red Hat Virtualization Hosts (RHVH) and Red Hat Enterprise Linux hosts from the Administration Portal. The procedure includes stopping and restarting the host.

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 reinstalls are performed at a time when the host's usage is relatively low.
- Ensure that the cluster 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 moving the host to maintenance.
- Ensure that the cluster contains more than one host before performing a reinstall. Do not attempt to reinstall all the hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.

Procedure

1. Click **Compute → Hosts** and select the host.
2. Click **Management → Maintenance**.
3. Click **Installation → Reinstall** to open the **Install Host** window.
4. Click the **Hosted Engine** tab and select **DEPLOY** from the drop-down list.
5. Click **OK** to reinstall the host.

Once successfully reinstalled, the host displays a status of **Up**. Any virtual machines that were migrated off the host can now be migrated back to it.

IMPORTANT

After a Red Hat Virtualization Host is successfully registered to the Red Hat Virtualization Manager and then reinstalled, it may erroneously appear in the Administration Portal with the status of **Install Failed**. Click **Management → Activate**, and the host will change to an **Up** status and be ready for use.

After reinstalling the self-hosted engine nodes, you can check the status of the new environment by running the following command on one of the nodes:

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

During the restoration, the old self-hosted engine storage domain was renamed, but was not removed from the new environment in case the restoration was faulty. After confirming that the environment is running normally, you can remove the old self-hosted engine storage domain.

7.4. REMOVING A STORAGE DOMAIN

You have a storage domain in your data center that you want to remove from the virtualized environment.

Procedure

Procedure

1. Click **Storage → Domains**.
2. Move the storage domain to maintenance mode and detach it:
    a. Click the storage domain's name to open the details view.
    b. Click the **Data Center** tab.
    c. Click **Maintenance**, then click **OK**.
    d. Click **Detach**, then click **OK**.
3. Click **Remove**.
4. Optionally select the **Format Domain, i.e. Storage Content will be lost!** check box to erase the content of the domain.
5. Click **OK**.

The storage domain is permanently removed from the environment.

CHAPTER 8. UPGRADING THE SELF-HOSTED ENGINE

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

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 8.1. Supported Upgrade Paths

Current Manager version	Target Manager version	Relevant section
3.6	4.2	Section 8.1, "Upgrading a Self-Hosted Engine from 3.6 to Red Hat Virtualization 4.2"
4.0	4.2	Section 8.2, "Upgrading a Self-Hosted Engine from 4.0 to Red Hat Virtualization 4.2"
4.1	4.2	Section 8.3, "Upgrading a Self-Hosted Engine from 4.1 to Red Hat Virtualization 4.2"
4.2.x	4.2.y	Section 4.7, "Updating the Manager Virtual Machine"

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.

8.1. UPGRADING A SELF-HOSTED ENGINE FROM 3.6 TO RED HAT VIRTUALIZATION 4.2

IMPORTANT

Use these instructions if your environment uses any Next Generation RHVH or Red Hat Enterprise Linux hosts.

If your environment uses only legacy RHEV-H 3.6 hosts, you must upgrade using the instructions in Appendix A, *Upgrading a RHEV-H 3.6 Self-Hosted Engine to a RHVH 4.2 Self-Hosted Engine*.

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

1. Place the environment in global maintenance mode
2. Update the 3.6 Manager to the latest version of 3.6
3. Upgrade the Manager from 3.6 to 4.0
4. Upgrade the Manager from 4.0 to 4.1

5. Upgrade the Manager from 4.1 to 4.2
6. Disable global maintenance mode
7. Upgrade the self-hosted engine nodes, and any standard hosts
8. Update the compatibility version of the clusters
9. Update the compatibility version of the data centers
10. Replace SHA-1 certificates with SHA-256 certificates

8.1.1. Enabling Global Maintenance Mode

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

Procedure

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

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

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

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

8.1.2. 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 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.

8.1.3. Upgrading the Self-hosted Engine 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 virtual machine to Red Hat Enterprise Linux 7 is not supported.

To upgrade a Red Hat Enterprise Virtualization 3.6 self-hosted engine environment to Red Hat Virtualization 4.0, you must use the upgrade utility that is provided with Red Hat Virtualization 4.0 to install a new Manager on Red Hat Enterprise Linux 7, and restore a backup of the 3.6 Manager database on the new Manager.

IMPORTANT

The upgrade utility builds a new Manager based on a template. Manual changes or custom configuration to the original Manager such as custom users, SSH keys, and monitoring must be reapplied manually on the new Manager.

Prerequisites

- All hosts in the environment must be running Red Hat Enterprise Linux 7.
- All data centers and clusters in the environment must have a compatibility version of 3.6.
- The **/var/tmp** directory must have at least 5 GB of free space to extract the appliance files. If it does not, you can specify a different directory or mount alternate storage that does have the required space. The VDSM user and KVM group must have read, write, and execute permissions on the directory.
- The self-hosted engine storage domain must have additional free space for the new appliance being deployed (50 GB by default). To increase the storage on iSCSI or Fibre Channel storage, you must manually extend the LUN size on the storage and then extend the storage domain

using the Manager. See Increasing iSCSI or FCP Storage in the *Red Hat Enterprise Virtualization 3.6 Administration Guide* for more information about resizing a LUN.

Procedure

1. On the host that is currently set as SPM and contains the Manager virtual machine, enable the required repository for Red Hat Virtualization 4.0:

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

2. Migrate all virtual machines except the Manager virtual machine to alternate hosts.

3. On the host, update the Manager virtual machine packages:

   ```
   # yum update ovirt-hosted-engine-setup rhevm-appliance
   ```

   If the **rhevm-appliance** package is missing, install it manually before updating **ovirt-hosted-engine-setup**.

   ```
   # yum install rhevm-appliance
   # yum update ovirt-hosted-engine-setup
   ```

4. Run the upgrade utility to upgrade the Manager virtual machine. If not already installed, install the **screen** package, which is available in the standard Red Hat Enterprise Linux repository:

   ```
   # yum install screen
   # screen
   # hosted-engine --upgrade-appliance
   ```

   You will be prompted to select the appliance if more than one is detected, and to create a backup of the Manager database and provide its full location.

If anything went wrong during the upgrade, power off the Manager by using the **hosted-engine --vm-poweroff** command, then roll back the upgrade by running **hosted-engine --rollback-upgrade**.

The backup created during the upgrade is not automatically deleted. You can manually delete it after confirming the upgrade was successful. The backup disks are labeled with **hosted-engine-backup-***.

8.1.4. 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.

8.1.5. 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.

8.1.6. Disabling Global Maintenance Mode

Procedure

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

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

2. Confirm that the environment is running:

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

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

8.1.7. 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 B, *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.

8.1.8. Changing the Cluster Compatibility Version

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

IMPORTANT

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

Procedure

1. 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.

8.1.9. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization 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.

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

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

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

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

```
            's;subject= \(.*\);\1;' \
    )"
    /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
        --name="${name}" \
        --password=mypass \
        --subject="${subject}" \
        --keep-key
done
```

6. Restart the **httpd** service:

```
# systemctl restart httpd
```

7. Log in to one of the self-hosted engine nodes and disable global maintenance:

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

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

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

Replacing All Signed Certificates with SHA-256

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

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

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

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

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

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

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

4. Replace the existing certificate with the new certificate:

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

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

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

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

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

For more details see Replacing the Red Hat Virtualization Manager SSL Certificate in the *Administration Guide*.

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

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

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

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

8. Restart the following services:

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

9. Log in to one of the self-hosted engine nodes and disable global maintenance:

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

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

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

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

a. In the Administration Portal, click **Compute → Hosts**.

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

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

d. Click **Management → Activate**.

8.2. UPGRADING A SELF-HOSTED ENGINE 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. Place the environment in global maintenance mode
2. Update the 4.0 Manager to the latest version of 4.0
3. Upgrade the Manager from 4.0 to 4.1
4. Upgrade the Manager from 4.1 to 4.2
5. Disable global maintenance mode
6. Upgrade the self-hosted engine nodes, and any standard hosts
7. Update the compatibility version of the clusters
8. Update the compatibility version of the data centers
9. Replace SHA-1 certificates with SHA-256 certificates

8.2.1. Enabling Global Maintenance Mode

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

Procedure

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

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

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

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

8.2.2. 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.

8.2.3. 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.

8.2.4. 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.

8.2.5. Disabling Global Maintenance Mode

Procedure

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

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

2. Confirm that the environment is running:

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

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

8.2.6. 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.

8.2.7. Changing the Cluster Compatibility Version

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

IMPORTANT

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

Procedure

1. 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.

8.2.8. 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.

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

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

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

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

6. Restart the **httpd** service:

```
# systemctl restart httpd
```

7. Log in to one of the self-hosted engine nodes and disable global maintenance:

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

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

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

Replacing All Signed Certificates with SHA-256

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

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

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

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

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

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

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

4. Replace the existing certificate with the new certificate:

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

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

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

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

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

   For more details see Replacing the Red Hat Virtualization Manager SSL Certificate in the *Administration Guide*.

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

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

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

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

8. Restart the following services:

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

9. Log in to one of the self-hosted engine nodes and disable global maintenance:

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

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

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

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

    a. In the Administration Portal, click **Compute** → **Hosts**.

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

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

    d. Click **Management** → **Activate**.

8.3. UPGRADING A SELF-HOSTED ENGINE FROM 4.1 TO RED HAT VIRTUALIZATION 4.2

Upgrading a self-hosted engine environment from version 4.1 to 4.2 involves the following steps:

1. Place the environment in global maintenance mode

2. Update the 4.1 Manager to the latest version of 4.1

3. Upgrade the Manager from 4.1 to 4.2

4. Disable global maintenance mode

5. Upgrade the self-hosted engine nodes, and any standard hosts

6. Update the compatibility version of the clusters

7. Update the compatibility version of the data centers

8. If you installed the technology preview version of Open Virtual Network (OVN) in 4.1, update the OVN provider's networking plugin

9. Replace SHA-1 certificates with SHA-256 certificates

8.3.1. Enabling Global Maintenance Mode

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

Procedure

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

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

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

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

8.3.2. 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.

8.3.3. 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.

8.3.4. Disabling Global Maintenance Mode

Procedure

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

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

2. Confirm that the environment is running:

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

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

8.3.5. 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.

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.

8.3.6. Changing the Cluster Compatibility Version

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

IMPORTANT

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

Procedure

1. 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.

8.3.7. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization 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.

8.3.8. 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**.

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

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

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

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

6. Restart the **httpd** service:

   ```
   # systemctl restart httpd
   ```

7. Log in to one of the self-hosted engine nodes and disable global maintenance:

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

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

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

Replacing All Signed Certificates with SHA-256

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

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

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

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

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

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

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

4. Replace the existing certificate with the new certificate:

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

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

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

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

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

   For more details see Replacing the Red Hat Virtualization Manager SSL Certificate in the *Administration Guide*.

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

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

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

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

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

8. Restart the following services:

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

9. Log in to one of the self-hosted engine nodes and disable global maintenance:

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

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

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

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

    a. In the Administration Portal, click **Compute → Hosts**.

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

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

    d. Click **Management → Activate**.

CHAPTER 9. MIGRATING THE SELF-HOSTED ENGINE DATABASE TO A REMOTE SERVER DATABASE

You can migrate the **engine** database of a self-hosted engine to a remote database server after the Red Hat Virtualization Manager has been initially configured. Use **engine-backup** to create a database backup and restore it on the new database server. This procedure assumes that the new database server has Red Hat Enterprise Linux 7 installed and the appropriate subscriptions configured. See Enabling the Red Hat Virtualization Manager Repositories in the *Installation Guide*.

To migrate Data Warehouse to a separate machine, see Migrating Data Warehouse to a Separate Machine in the *Data Warehouse Guide*.

Migrating the Database

1. Log in to a self-hosted engine node and place the environment into **global** maintenance mode. This disables the High Availability agents and prevents the Manager virtual machine from being migrated during the procedure:

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

2. Log in to the Red Hat Virtualization Manager machine and stop the **ovirt-engine** service so that it does not interfere with the engine backup:

   ```
   # systemctl stop ovirt-engine.service
   ```

3. Create the **engine** database backup:

   ```
   # engine-backup --scope=files --scope=db --mode=backup --file=file_name --
   log=backup_log_name
   ```

4. Copy the backup file to the new database server:

   ```
   # scp /tmp/engine.dump root@new.database.server.com:/tmp
   ```

5. Log in to the new database server and install **engine-backup**:

   ```
   # yum install ovirt-engine-tools-backup
   ```

6. Restore the database on the new database server. *file_name* is the backup file copied from the Manager.

   ```
   # engine-backup --mode=restore --scope=files --scope=db --file=file_name --
   log=restore_log_name --provision-db --no-restore-permissions
   ```

7. Now that the database has been migrated, start the **ovirt-engine** service:

   ```
   # systemctl start ovirt-engine.service
   ```

8. Log in to a self-hosted engine node and turn off maintenance mode, enabling the High Availability agents:

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

APPENDIX A. UPGRADING A RHEV-H 3.6 SELF-HOSTED ENGINE TO A RHVH 4.2 SELF-HOSTED ENGINE

To upgrade a Red Hat Enterprise Virtualization 3.6 self-hosted engine environment that contains only Red Hat Enterprise Virtualization Hypervisors (RHEV-H) to Red Hat Virtualization 4.2, you must remove the hosts and install Red Hat Virtualization Host (RHVH) instead.

Self-hosted engine nodes in Red Hat Enterprise Virtualization 3.6 are added using the **hosted-engine --deploy** command, which cannot be used to add RHVH 4.2 as an additional node, and self-hosted engine nodes in Red Hat Virtualization 4.2 are added using the UI, which is not available in Red Hat Enterprise Virtualization 3.6. Therefore, to upgrade the environment from 3.6 to 4.2, you must first install a self-hosted engine node running RHVH 4.0, where adding more nodes using the **hosted-engine --deploy** command is deprecated but still available.

Alternatively, you can install a 3.6 version of RHVH in the 3.6 environment and perform a standard stepped upgrade from 3.6 to 4.0, and 4.0 to 4.1. See Red Hat Virtualization Hosts in the *Red Hat Enterprise Virtualization 3.6 Self-Hosted Engine Guide* for more information.

NOTE

This scenario does not impact self-hosted engine environments that contain some (or only) Red Hat Enterprise Linux or Next Generation RHVH self-hosted engine nodes, as they can be updated without being removed from the environment.

IMPORTANT

Before upgrading the Manager virtual machine, ensure the **/var/tmp** directory contains 5 GB free space to extract the appliance files. If it does not, you can specify a different directory or mount alternate storage that does have the required space. The VDSM user and KVM group must have read, write, and execute permissions on the directory.

Upgrading from a Red Hat Enterprise Virtualization 3.6 self-hosted engine environment with RHEV-H 3.6 hosts to a Red Hat Virtualization 4.2 environment with RHVH 4.2 hosts involves the following key steps:

- Install a new RHVH 4.0 host and add it to the 3.6 self-hosted engine environment. The new host can be an existing RHEV-H 3.6 host removed from the environment and reinstalled with RHVH 4.0.
- Upgrade the Manager from 3.6 to 4.0.
- Remove the rest of the RHEV-H 3.6 hosts and reinstall them with RHVH 4.2.
- Add the RHVH 4.2 hosts to the 4.0 environment.
- Upgrade the Manager from 4.0 to 4.1.
- Upgrade the Manager from 4.1 to 4.2.
- Upgrade the remaining RHVH 4.0 host to RHVH 4.2.

Upgrading a RHEV-H 3.6 Self-Hosted Engine to a RHVH 4.2 Self-Hosted Engine

1. If you are reusing an existing RHEV-H 3.6 host, remove it from the 3.6 environment. See Removing a Host from a Self-Hosted Engine Environment .

2. Upgrade the environment from 3.6 to 4.0 using the instructions in Upgrading a RHEV-H-Based Self-Hosted Engine Environment in the *Red Hat Virtualization 4.0 Self-Hosted Engine Guide* . These instructions include installing a RHVH 4.0 host.

3. Upgrade each remaining RHEV-H 3.6 host directly to RHVH 4.2:

   a. Remove the host from the self-hosted engine environment. See Removing a Host from a Self-Hosted Engine Environment.

   b. Reinstall the host with RHVH 4.2. See Installing Red Hat Virtualization Host in the *Installation Guide*.

   c. Add the host to the 4.0 environment. See Installing Additional Hosts to a Self-Hosted Environment in the *Red Hat Virtualization 4.0 Self-Hosted Engine Guide* .

4. Upgrade the Manager from 4.0 to 4.1:

   a. In the Administration Portal, right-click a self-hosted engine node and select **Enable Global HA Maintenance**.
      Wait a few minutes and ensure that you see **Hosted Engine HA: Global Maintenance Enabled** in the **General** tab.

   b. Use the instructions in Upgrading to Red Hat Virtualization Manager 4.1 .

5. Upgrade the Manager from 4.1 to 4.2 and then upgrade the final remaining RHVH 4.0 host to 4.2 using the instructions in Upgrading a Self-Hosted Engine from 4.1 to Red Hat Virtualization 4.2.

APPENDIX B. 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.