Red Hat Virtualization 4.0

Installation Guide

Installing Red Hat Virtualization

Last Updated: 2019-02-21

Red Hat Virtualization 4.0 Installation Guide

Installing Red Hat Virtualization

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

Legal Notice

Abstract

A comprehensive guide to installing Red Hat Virtualization.

Table of Contents

PART I. INTRODUCTION TO RED HAT VIRTUALIZATION

CHAPTER 1. INTRODUCTION TO RED HAT VIRTUALIZATION

Red Hat Virtualization is an enterprise-grade server and desktop virtualization platform built on Red Hat Enterprise Linux. This guide covers:

- The installation and configuration of a Red Hat Virtualization Manager.
- The installation and configuration of hosts.
- Attach existing FCP storage to your Red Hat Virtualization environment. More storage options can be found in the Administration Guide.

Table 1.1. Red Hat Virtualization Key Components

Component Name	Description
Red Hat Virtualization Manager	A server that manages and provides access to the resources in the environment.
Hosts	Hosts are servers that provide the processing capabilities and memory resources used to run virtual machines.
Storage	Storage is used to store the data associated with virtual machines.

IMPORTANT

It is important to synchronize the system clocks of the hosts, Manager, and other servers in the environment to avoid potential timing or authentication issues. To do this, configure the Network Time Protocol (NTP) on each system to synchronize with the same NTP server.

CHAPTER 2. SYSTEM REQUIREMENTS

Hardware certification for Red Hat Virtualization is covered by the hardware certification for Red Hat Enterprise Linux. For more information, see https://access.redhat.com/solutions/725243.

2.1. RED HAT VIRTUALIZATION MANAGER REQUIREMENTS

2.1.1. Hardware Requirements

The minimum and recommended hardware requirements outlined here are based on a typical small to medium sized installation. The exact requirements vary between deployments based on sizing and load.

The Red Hat Virtualization Manager runs on Red Hat Enterprise Linux. To confirm whether or not specific hardware items are certified for use with Red Hat Enterprise Linux, see https://access.redhat.com/ecosystem/#certifiedHardware.

Table 2.1. Red Hat Virtualization Manager Hardware Requirements

Resource	Minimum	Recommended
CPU	A dual core CPU.	A quad core CPU or multiple dual core CPUs.
Memory	4 GB of available system RAM if Data Warehouse is not installed and if memory is not being consumed by existing processes.	16 GB of system RAM.
Hard Disk	25 GB of locally accessible, writable, disk space.	50 GB of locally accessible, writable, disk space. You can use the RHEV Manager History Database Size Calculator to calculate the appropriate disk space to have for the Manager history database size.
Network Interface	1 Network Interface Card (NIC) with bandwidth of at least 1 Gbps.	1 Network Interface Card (NIC) with bandwidth of at least 1 Gbps.

2.1.2. Browser Requirements

The following browser versions and operating systems can be used to access the Administration Portal and the User Portal.

Browser support is divided into tiers:

- Tier 1: Browser and operating system combinations that are fully tested and fully supported. Red Hat Engineering is committed to fixing issues with browsers on this tier.
- Tier 2: Browser and operating system combinations that are partially tested, and are likely to work. Limited support is provided for this tier. Red Hat Engineering will attempt to fix issues with browsers on this tier.
- Tier 3: Browser and operating system combinations that are not tested, but may work. Minimal support is provided for this tier. Red Hat Engineering will attempt to fix only minor issues with browsers on this tier.

Table 2.2. Browser Requirements

Support Tier	Operating System Family	Browser	Portal Access
Tier 1	Red Hat Enterprise Linux	Mozilla Firefox Extended Support Release (ESR) version	Administration Portal and User Portal
Tier 2	Windows	Internet Explorer 10 or later	Administration Portal and User Portal
	Any	Most recent version of Google Chrome or Mozilla Firefox	Administration Portal and User Portal
Tier 3	Any	Earlier versions of Google Chrome or Mozilla Firefox	Administration Portal and User Portal
	Any	Other browsers	Administration Portal and User Portal

2.1.3. Client Requirements

Virtual machine consoles can only be accessed using supported Remote Viewer (virt-viewer) clients on Red Hat Enterprise Linux and Windows. To install virt-viewer, see Installing Supported Components in the *Virtual Machine Management Guide*. Installing virt-viewer requires Administrator privileges.

SPICE console access is only available on other operating systems, such as OS X, through the unsupported SPICE HTML5 browser client.

Supported QXL drivers are available on Red Hat Enterprise Linux, Windows XP, and Windows 7.

SPICE support is divided into tiers:

- Tier 1: Operating systems on which remote-viewer has been fully tested and is supported.

- Tier 2: Operating systems on which remote-viewer is partially tested and is likely to work. Limited support is provided for this tier. Red Hat Engineering will attempt to fix issues with remote-viewer on this tier.

Table 2.3. Client Operating System SPICE Support

Support Tier	Operating System	SPICE Support
Tier 1	Red Hat Enterprise Linux 7	Fully supported on Red Hat Enterprise Linux 7.2 and above
	Microsoft Windows 7	Fully supported on Microsoft Windows 7
Tier 2	Microsoft Windows 8	Supported when spice-vdagent is running on these guest operating systems
	Microsoft Windows 10	Supported when spice-vdagent is running on these guest operating systems

2.1.4. Operating System Requirements

The Red Hat Virtualization Manager must be installed on a base installation of Red Hat Enterprise Linux 7 that has been updated to the latest minor release. Do not install any additional packages after the base installation because they may cause dependency issues when attempting to install the packages required by the Manager.

2.1.5. DNS Requirements

The Red Hat Virtualization Manager and all network communication requires reverse DNS lookup and the existence of a PTR record to avoid significant performance degredation.

NOTE

An entry in the **/etc/hosts** file is not sufficient because it does not provide reverse DNS lookup.

2.2. HYPERVISOR REQUIREMENTS

2.2.1. CPU Requirements

All CPUs must have support for the Intel® 64 or AMD64 CPU extensions, and the AMD-V™ or Intel VT® hardware virtualization extensions enabled. Support for the No eXecute flag (NX) is also required.

Table 2.4. Supported Hypervisor CPU Models

AMD	Intel	IBM
AMD Opteron G1	Intel Conroe	IBM POWER8
AMD Opteron G2	Intel Penryn	
AMD Opteron G3	Intel Nehalem	
AMD Opteron G4	Intel Westmere	
AMD Opteron G5	Intel Sandybridge	
	Intel Haswell	

Procedure 2.1. Checking if a Processor Supports the Required Flags

You must enable Virtualization in the BIOS. Power off and reboot the host after this change to ensure that the change is applied.

1. At the Red Hat Enterprise Linux or Red Hat Virtualization Host boot screen, press any key and select the **Boot** or **Boot with serial console** entry from the list.
2. Press **Tab** to edit the kernel parameters for the selected option.
3. Ensure there is a **Space** after the last kernel parameter listed, and append the **rescue** parameter.
4. Press **Enter** to boot into rescue mode.
5. At the prompt which appears, determine that your processor has the required extensions and that they are enabled by running this command:

   ```
   # grep -E 'svm|vmx' /proc/cpuinfo | grep nx
   ```

   If any output is shown, then the processor is hardware virtualization capable. If no output is shown, then it is still possible that your processor supports hardware virtualization. In some circumstances manufacturers disable the virtualization extensions in the BIOS. If you believe this to be the case, consult the system's BIOS and the motherboard manual provided by the manufacturer.

2.2.2. Memory Requirements

The amount of RAM required varies depending on guest operating system requirements, guest application requirements, and memory activity and usage of guests. You also need to take into account that KVM is able to overcommit physical RAM for virtualized guests. This allows for provisioning of guests with RAM requirements greater than what is physically present, on the basis that the guests are not all concurrently at peak load. KVM does this by only allocating RAM for guests as required and shifting underutilized guests into swap.

Table 2.5. Memory Requirements

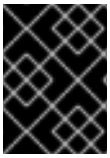
Minimum	Maximum
2 GB of RAM	2 TB of RAM

2.2.3. Storage Requirements

Hosts require local storage to store configuration, logs, kernel dumps, and for use as swap space. The minimum storage requirements of Red Hat Virtualization Host are documented in this section. The storage requirements for Red Hat Enterprise Linux hosts vary based on the amount of disk space used by their existing configuration but are expected to be greater than those of Red Hat Virtualization Host.

Table 2.6. Red Hat Virtualization Host Minimum Storage Requirements

/	/boot	/var	swap	Minimum Total
6 GB	1 GB	15 GB	1 GB	23 GB



IMPORTANT

If you are also installing the RHV-M Virtual Appliance for self-hosted engine installation, the /var partition must be at least 60 GB.

For the recommended swap size, see https://access.redhat.com/solutions/15244.

2.2.4. PCI Device Requirements

Hosts must have at least one network interface with a minimum bandwidth of 1 Gbps. It is recommended that each host have two network interfaces with one dedicated to support network intensive activities such as virtual machine migration. The performance of such operations are limited by the bandwidth available.

2.2.5. Hardware Considerations For Device Assignment

If you plan to implement device assignment and PCI passthrough so that a virtual machine can use a specific PCIe device from a host, ensure the following requirements are met:

- CPU must support IOMMU (for example, VT-d or AMD-Vi). IBM POWER8 supports IOMMU by default.
- Firmware must support IOMMU.
- CPU root ports used must support ACS or ACS-equivalent capability.
- PCIe device must support ACS or ACS-equivalent capability.
- It is recommended that all PCIe switches and bridges between the PCIe device and the root port should support ACS. For example, if a switch does not support ACS, all devices behind that switch share the same IOMMU group, and can only be assigned to the same virtual machine.
- For GPU support, Red Hat Enterprise Linux 7 supports PCI device assignment of

NVIDIA K-Series Quadro (model 2000 series or higher), GRID, and Tesla as non-VGA graphics devices. Currently up to two GPUs may be attached to a virtual machine in addition to one of the standard, emulated VGA interfaces. The emulated VGA is used for pre-boot and installation and the NVIDIA GPU takes over when the NVIDIA graphics drivers are loaded. Note that the NVIDIA Quadro 2000 is not supported, nor is the Quadro K420 card.

Refer to vendor specification and datasheets to confirm that hardware meets these requirements. After you have installed a host, see Appendix G, *Configuring a Host for PCI Passthrough* for more information on how to enable the host hardware and software for device passthrough.

To implement SR-IOV, see https://access.redhat.com/documentation/en/red-hat-virtualization/4.0/single/hardware-considerations-for-implementing-sr-iov/ for more information.

The **`lspci -v`** command can be used to print information for PCI devices already installed on a system.

2.3. FIREWALLS

2.3.1. Red Hat Virtualization Manager Firewall Requirements

The Red Hat Virtualization Manager requires that a number of ports be opened to allow network traffic through the system's firewall. The **`engine-setup`** script can configure the firewall automatically, but this overwrites any pre-existing firewall configuration.

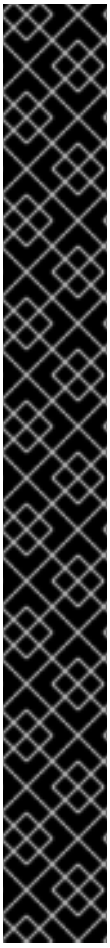
Where an existing firewall configuration exists, you must manually insert the firewall rules required by the Manager instead. The **`engine-setup`** command saves a list of the**`iptables`** rules required in the **`/usr/share/ovirt-engine/conf/iptables.example`** file.

The firewall configuration documented here assumes a default configuration. Where non-default HTTP and HTTPS ports are chosen during installation, adjust the firewall rules to allow network traffic on the ports that were selected - not the default ports (**`80`** and **`443`**) listed here.

Table 2.7. Red Hat Virtualization Manager Firewall Requirements

Port(s)	Protocol	Source	Destination	Purpose
-	ICMP	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Red Hat Virtualization Manager	When registering to the Red Hat Virtualization Manager, virtualization hosts send an ICMP ping request to the Manager to confirm that it is online.

Port(s)	Protocol	Source	Destination	Purpose
22	TCP	System(s) used for maintenance of the Manager including backend configuration, and software upgrades.	Red Hat Virtualization Manager	Secure Shell (SSH) access. Optional.
2222	TCP	Clients accessing virtual machine serial consoles.	Red Hat Virtualization Manager	Secure Shell (SSH) access to enable connection to virtual machine serial consoles.
80, 443	TCP	Administration Portal clients User Portal clients Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s) REST API clients	Red Hat Virtualization Manager	Provides HTTP and HTTPS access to the Manager.
6100	TCP	Administration Portal clients User Portal clients	Red Hat Virtualization Manager	Provides websocket proxy access for web-based console clients (**noVNC** and **spice-html5**) when the websocket proxy is running on the Manager. If the websocket proxy is running on a different host, however, this port is not used.
7410	UDP	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Red Hat Virtualization Manager	Must be open for the Manager to receive Kdump notifications.



IMPORTANT

In environments where the Red Hat Virtualization Manager is also required to export NFS storage, such as an ISO Storage Domain, additional ports must be allowed through the firewall. Grant firewall exceptions for the ports applicable to the version of NFS in use:

NFSv4

- TCP port **2049** for NFS.

NFSv3

- TCP and UDP port **2049** for NFS.
- TCP and UDP port **111** (**rpcbind**/**sunrpc**).
- TCP and UDP port specified with **MOUNTD_PORT="*port*"**
- TCP and UDP port specified with **STATD_PORT="*port*"**
- TCP port specified with **LOCKD_TCPPORT="*port*"**
- UDP port specified with **LOCKD_UDPPORT="*port*"**

The **MOUNTD_PORT**, **STATD_PORT**, **LOCKD_TCPPORT**, and **LOCKD_UDPPORT** ports are configured in the **/etc/sysconfig/nfs** file.

2.3.2. Hypervisor Firewall Requirements

Red Hat Enterprise Linux hosts and Red Hat Virtualization Hosts (RHVH) require a number of ports to be opened to allow network traffic through the system's firewall. In the case of the Red Hat Virtualization Host these firewall rules are configured automatically. For Red Hat Enterprise Linux hosts however it is necessary to manually configure the firewall.

Table 2.8. Virtualization Host Firewall Requirements

Port(s)	Protocol	Source	Destination	Purpose
22	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Secure Shell (SSH) access. Optional.
2223	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Secure Shell (SSH) access to enable connection to virtual machine serial consoles.

Port(s)	Protocol	Source	Destination	Purpose
161	UDP	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Red Hat Virtualization Manager	Simple network management protocol (SNMP). Only required if you want Simple Network Management Protocol traps sent from the host to one or more external SNMP managers. Optional.
5900 - 6923	TCP	Administration Portal clients User Portal clients	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Remote guest console access via VNC and SPICE. These ports must be open to facilitate client access to virtual machines.
5989	TCP, UDP	Common Information Model Object Manager (CIMOM)	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Used by Common Information Model Object Managers (CIMOM) to monitor virtual machines running on the host. Only required if you want to use a CIMOM to monitor the virtual machines in your virtualization environment. Optional.
9090	TCP	Red Hat Virtualization Manager Client machines	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Cockpit user interface access. Optional.

Port(s)	Protocol	Source	Destination	Purpose
16514	TCP	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Virtual machine migration using **`libvirt`**.
49152 - 49216	TCP	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Virtual machine migration and fencing using VDSM. These ports must be open facilitate both automated and manually initiated migration of virtual machines.
54321	TCP	Red Hat Virtualization Manager Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	Red Hat Virtualization Host(s) Red Hat Enterprise Linux host(s)	VDSM communications with the Manager and other virtualization hosts.

2.3.3. Directory Server Firewall Requirements

Red Hat Virtualization requires a directory server to support user authentication. A number of ports must be opened in the directory server's firewall to support GSS-API authentication as used by the Red Hat Virtualization Manager.

Table 2.9. Host Firewall Requirements

Port(s)	Protocol	Source	Destination	Purpose
88, 464	TCP, UDP	Red Hat Virtualization Manager	Directory server	Kerberos authentication.
389, 636	TCP	Red Hat Virtualization Manager	Directory server	Lightweight Directory Access Protocol (LDAP) and LDAP over SSL.

2.3.4. Database Server Firewall Requirements

Red Hat Virtualization supports the use of a remote database server. If you plan to use a remote database server with Red Hat Virtualization then you must ensure that the remote database server allows connections from the Manager.

Table 2.10. Host Firewall Requirements

Port(s)	Protocol	Source	Destination	Purpose
5432	TCP, UDP	Red Hat Virtualization Manager	PostgreSQL database server	Default port for PostgreSQL database connections.

If you plan to use a local database server on the Manager itself, which is the default option provided during installation, then no additional firewall rules are required.

PART II. INSTALLING THE RED HAT VIRTUALIZATION MANAGER

CHAPTER 3. RED HAT VIRTUALIZATION MANAGER

3.1. SUBSCRIBING TO THE REQUIRED ENTITLEMENTS

Once you have installed a Red Hat Enterprise Linux base operating system and made sure the system meets the requirements listed in the previous chapter, you must register the system with Red Hat Subscription Manager, and subscribe to the required entitlements to install the Red Hat Virtualization Manager packages.

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 note down the pool IDs.

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

3. Use the pool IDs located in the previous step to attach the entitlements to the system:

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

NOTE

To find out what subscriptions are currently attached, run:

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

To list all enabled repositories, run:

```
# yum repolist
```

4. Disable all existing repositories:

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

5. Enable the required repositories:

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

You have now subscribed your system to the required entitlements. Proceed to the next section to install the Red Hat Virtualization Manager packages.

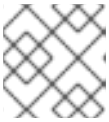
3.2. INSTALLING THE RED HAT VIRTUALIZATION MANAGER PACKAGES

Before you can configure and use the Red Hat Virtualization Manager, you must install the rhevm package and dependencies.

Procedure 3.1. Installing the Red Hat Virtualization Manager Packages

1. To ensure all packages are up to date, run the following command on the machine where you are installing the Red Hat Virtualization Manager:

```
# yum update
```



NOTE

Reboot the machine if any kernel related packages have been updated.

2. Run the following command to install the rhevm package and dependencies.

```
# yum install rhevm
```

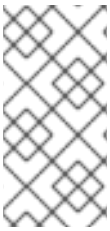
Proceed to the next step to configure your Red Hat Virtualization Manager.

3.3. CONFIGURING THE RED HAT VIRTUALIZATION MANAGER

After you have installed the rhevm package and dependencies, you must configure the Red Hat Virtualization Manager using the **engine-setup** command. This command asks you a series of questions and, after you provide the required values for all questions, applies that configuration and starts the **ovirt-engine** service.

By default, **engine-setup** creates and configures the Manager database locally on the Manager machine. Alternatively, you can configure the Manager to use a remote database or a manually-configured local database; however, you must set up that database before running **engine-setup**. To set up a remote database seeAppendix D, *Preparing a Remote PostgreSQL Database for Use with the Red Hat Virtualization Manager*. To set up a manually-configured local database, see Appendix E, *Preparing a Local Manually-Configured PostgreSQL Database for Use with the Red Hat Virtualization Manager*.

By default, **engine-setup** will configure a websocket proxy on the Manager. However, for security and performance reasons, the user can choose to configure it on a separate host. See Appendix F, *Installing a Websocket Proxy on a Separate Machine* for instructions.



NOTE

The **engine-setup** command guides you through several distinct configuration stages, each comprising several steps that require user input. Suggested configuration defaults are provided in square brackets; if the suggested value is acceptable for a given step, press **Enter** to accept that value.

Procedure 3.2. Configuring the Red Hat Virtualization Manager

1. Run the **engine-setup** command to begin configuration of the Red Hat Virtualization Manager:

```
# engine-setup
```

2. Press **Enter** to configure the Manager:

```
Configure Engine on this host (Yes, No) [Yes]:
```

3. Optionally allow **engine-setup** to configure the Image I/O Proxy to allow the Manager to upload virtual disk images into storage domains. See Uploading a Disk Image to a Storage Domain in the *Administration Guide* for more information.

```
Configure Image I/O Proxy on this host? (Yes, No) [Yes]:
```

4. Optionally allow **engine-setup** to configure a websocket proxy server for allowing users to connect to virtual machines via the noVNC or HTML 5 consoles:

```
Configure WebSocket Proxy on this machine? (Yes, No) [Yes]:
```

To configure the websocket proxy on a separate machine, select **No** and refer to Appendix F, *Installing a Websocket Proxy on a Separate Machine* for configuration instructions.

5. Choose whether to configure Data Warehouse on the Manager machine.

```
Please note: Data Warehouse is required for the engine. If you
choose to not configure it on this host, you have to configure it on
a remote host, and then configure the engine on this host so that it
can access the database of the remote Data Warehouse host.
Configure Data Warehouse on this host (Yes, No) [Yes]:
```

To configure Data Warehouse on a separate machine, select **No** and see Installing and Configuring Data Warehouse on a Separate Machine in the *Data Warehouse Guide* for installation and configuration instructions.

6. Optionally allow access to a virtual machines's serial console from the command line.

```
Configure VM Console Proxy on this host (Yes, No) [Yes]:
```

Additional configuration is required on the client machine to use this feature. See Opening a Serial Console to a Virtual Machine in the *Virtual Machine Management Guide*.

7. Press **Enter** to accept the automatically detected hostname, or enter an alternative hostname and press **Enter**. Note that the automatically detected hostname may be incorrect if you are using virtual hosts.

```
Host fully qualified DNS name of this server [autodetected host
name]:
```

8. The **engine-setup** command checks your firewall configuration and offers to modify

that configuration to open the ports used by the Manager for external communication such as TCP ports 80 and 443. If you do not allow **engine-setup** to modify your firewall configuration, then you must manually open the ports used by the Manager.

```
Setup can automatically configure the firewall on this system.
Note: automatic configuration of the firewall may overwrite current
settings.
Do you want Setup to configure the firewall? (Yes, No) [Yes]:
```

If you choose to automatically configure the firewall, and no firewall managers are active, you are prompted to select your chosen firewall manager from a list of supported options. Type the name of the firewall manager and press **Enter**. This applies even in cases where only one option is listed.

9. Choose to use either a local or remote PostgreSQL database as the Data Warehouse database:

```
Where is the DWH database located? (Local, Remote) [Local]:
```

- If you select **Local**, the **engine-setup** command can configure your database automatically (including adding a user and a database), or it can connect to a preconfigured local database:

```
Setup can configure the local postgresql server automatically for
the DWH to run. This may conflict with existing applications.
Would you like Setup to automatically configure postgresql and
create DWH database, or prefer to perform that manually?
(Automatic, Manual) [Automatic]:
```

  a. If you select **Automatic** by pressing **Enter**, no further action is required here.

  b. If you select **Manual**, input the following values for the manually-configured local database:

```
DWH database secured connection (Yes, No) [No]:
DWH database name [ovirt_engine_history]:
DWH database user [ovirt_engine_history]:
DWH database password:
```

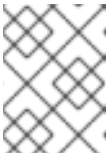
NOTE

engine-setup requests these values after the Manager database is configured in the next step.

- If you select **Remote**, input the following values for the preconfigured remote database host:

```
DWH database host [localhost]:
DWH database port [5432]:
DWH database secured connection (Yes, No) [No]:
```

```
DWH database name [ovirt_engine_history]:
DWH database user [ovirt_engine_history]:
DWH database password:
```



NOTE

engine-setup requests these values after the Manager database is configured in the next step.

10. Choose to use either a local or remote PostgreSQL database as the Manager database:

```
Where is the Engine database located? (Local, Remote) [Local]:
```

- If you select **Local**, the **engine-setup** command can configure your database automatically (including adding a user and a database), or it can connect to a preconfigured local database:

```
Setup can configure the local postgresql server automatically for
the engine to run. This may conflict with existing applications.
Would you like Setup to automatically configure postgresql and
create Engine database, or prefer to perform that manually?
(Automatic, Manual) [Automatic]:
```

  a. If you select **Automatic** by pressing **Enter**, no further action is required here.

  b. If you select **Manual**, input the following values for the manually-configured local database:

```
Engine database secured connection (Yes, No) [No]:
Engine database name [engine]:
Engine database user [engine]:
Engine database password:
```

- If you select **Remote**, input the following values for the preconfigured remote database host:

```
Engine database host [localhost]:
Engine database port [5432]:
Engine database secured connection (Yes, No) [No]:
Engine database name [engine]:
Engine database user [engine]:
Engine database password:
```

11. Set a password for the automatically created administrative user of the Red Hat Virtualization Manager:

```
Engine admin password:
Confirm engine admin password:
```

12. Select **Gluster**, **Virt**, or **Both**:

```
Application mode (Both, Virt, Gluster) [Both]:
```

Both offers the greatest flexibility. In most cases, select **Both**. Virt application mode allows you to run virtual machines in the environment; Gluster application mode only allows you to manage GlusterFS from the Administration Portal.

13. Set the default value for the **wipe_after_delete** flag, which wipes the blocks of a virtual disk when the disk is deleted.

```
Default SAN wipe after delete (Yes, No) [No]:
```

14. The Manager uses certificates to communicate securely with its hosts. This certificate can also optionally be used to secure HTTPS communications with the Manager. Provide the organization name for the certificate:

```
Organization name for certificate [autodetected domain-based name]:
```

15. Optionally allow **engine-setup** to make the landing page of the Manager the default page presented by the Apache web server:

```
Setup can configure the default page of the web server to present
the application home page. This may conflict with existing
applications.
Do you wish to set the application as the default web page of the
server? (Yes, No) [Yes]:
```

16. By default, external SSL (HTTPS) communication with the Manager is secured with the self-signed certificate created earlier in the configuration to securely communicate with hosts. Alternatively, choose another certificate for external HTTPS connections; this does not affect how the Manager communicates with hosts:

```
Setup can configure apache to use SSL using a certificate issued
from the internal CA.
 Do you wish Setup to configure that, or prefer to perform that
manually? (Automatic, Manual) [Automatic]:
```

17. Optionally create an NFS share on the Manager to use as an ISO storage domain. The local ISO domain provides a selection of images that can be used in the initial setup of virtual machines:

    a.
    ```
    Configure an NFS share on this server to be used as an ISO
    Domain? (Yes, No) [Yes]:
    ```

    b. Specify the path for the ISO domain:

    ```
    Local ISO domain path [/var/lib/exports/iso]:
    ```

    c. Specify the networks or hosts that require access to the ISO domain:

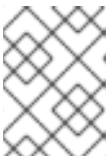
    ```
    Local ISO domain ACL: 10.1.2.0/255.255.255.0(rw)
    host01.example.com(rw) host02.example.com(rw)
    ```

The example above allows access to a single /24 network and two specific hosts. See the **exports(5)** man page for further formatting options.

d. Specify a display name for the ISO domain:

```
Local ISO domain name [ISO_DOMAIN]:
```

18. Choose how long Data Warehouse will retain collected data:



NOTE

This step is skipped if you chose not to configure Data Warehouse on the Manager machine.

```
Please choose Data Warehouse sampling scale:
(1) Basic
(2) Full
(1, 2)[1]:
```

Full uses the default values for the data storage settings listed in the *Data Warehouse Guide* (recommended when Data Warehouse is installed on a remote host).

Basic reduces the values of **DWH_TABLES_KEEP_HOURLY** to **720** and **DWH_TABLES_KEEP_DAILY** to **0**, easing the load on the Manager machine (recommended when the Manager and Data Warehouse are installed on the same machine).

19. Review the installation settings, and press **Enter** to accept the values and proceed with the installation:

```
Please confirm installation settings (OK, Cancel) [OK]:
```

20. If you intend to link your Red Hat Virtualization environment with a directory server, configure the date and time to synchronize with the system clock used by the directory server to avoid unexpected account expiry issues. See Synchronizing the System Clock with a Remote Server in the *Red Hat Enterprise Linux System Administrator's Guide* for more information.

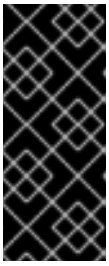
When your environment has been configured, **engine-setup** displays details about how to access your environment. If you chose to manually configure the firewall, **engine-setup** provides a custom list of ports that need to be opened, based on the options selected during setup. The **engine-setup** command also saves your answers to a file that can be used to reconfigure the Manager using the same values, and outputs the location of the log file for the Red Hat Virtualization Manager configuration process.

Proceed to the next section to connect to the Administration Portal as the **admin@internal** user. Then, proceed with setting up hosts, and attaching storage.

3.4. LOGGING IN TO AND OUT OF THE ADMINISTRATION PORTAL

Access the Administration Portal using a web browser.

1. In a web browser, navigate to **https://*your-manager-fqdn*/ovirt-engine**, replacing *your-manager-fqdn* with the fully qualified domain name that you provided during installation.



IMPORTANT

The first time that you connect to the Administration Portal, you are prompted to trust the certificate being used to secure communications between your browser and the web server. You must accept this certificate. Refer to the instructions to install the certificate authority in Firefox, Internet Explorer, or Google Chrome.

2. Click **Administration Portal**. An SSO login page displays. SSO login enables you to log in to the Administration and User Portals at the same time.

3. Enter your **User Name** and **Password**. If you are logging in for the first time, use the user name **admin** in conjunction with the password that you specified during installation.

4. Select the domain against which to authenticate from the **Domain** list. If you are logging in using the internal **admin** user name, select the **internal** domain.

5. Click **Log In**.

6. You can view the Administration Portal in multiple languages. The default selection will be chosen based on the locale settings of your web browser. If you would like to view the Administration Portal in a language other than the default, select your preferred language from the drop-down list on the welcome page.

To log out of the Red Hat Virtualization Administration Portal, click your user name in the header bar and click **Sign Out**. You are logged out of all portals and the Manager welcome screen displays.

The next chapter contains additional Manager related tasks which are optional. If the tasks are not applicable to your environment, proceed to Part III, “Installing Hosts”.

CHAPTER 4. RED HAT VIRTUALIZATION MANAGER RELATED TASKS

4.1. REMOVING THE RED HAT VIRTUALIZATION MANAGER

You can use the **engine-cleanup** command to remove specific components or all components of the Red Hat Virtualization Manager.

NOTE

A backup of the engine database and a compressed archive of the PKI keys and configuration are always automatically created. These files are saved under **/var/lib/ovirt-engine/backups/**, and include the date and **engine-** and **engine-pki-** in their file names respectively.

Procedure 4.1. Removing the Red Hat Virtualization Manager

1. Run the following command on the machine on which the Red Hat Virtualization Manager is installed:

```
# engine-cleanup
```

2. You are prompted whether to remove all Red Hat Virtualization Manager components:
   - Type **Yes** and press **Enter** to remove all components:

```
Do you want to remove all components? (Yes, No) [Yes]:
```

   - Type **No** and press **Enter** to select the components to remove. You can select whether to retain or remove each component individually:

```
Do you want to remove Engine database content? All data will be
lost (Yes, No) [No]:
Do you want to remove PKI keys? (Yes, No) [No]:
Do you want to remove PKI configuration? (Yes, No) [No]:
Do you want to remove Apache SSL configuration? (Yes, No) [No]:
```

3. You are given another opportunity to change your mind and cancel the removal of the Red Hat Virtualization Manager. If you choose to proceed, the **ovirt-engine** service is stopped, and your environment's configuration is removed in accordance with the options you selected.

```
During execution engine service will be stopped (OK, Cancel) [OK]:
ovirt-engine is about to be removed, data will be lost (OK, Cancel)
[Cancel]:OK
```

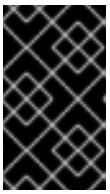
4. Remove the Red Hat Virtualization packages:

```
# yum remove rhevm* vdsm-bootstrap
```

4.2. CONFIGURING A LOCAL REPOSITORY FOR OFFLINE RED HAT VIRTUALIZATION MANAGER INSTALLATION

To install Red Hat Virtualization Manager on a system that does not have a direct connection to the Content Delivery Network, download the required packages on a system that has Internet access, then create a repository that can be shared with the offline Manager machine. The system hosting the repository must be connected to the same network as the client systems where the packages are to be installed.

1. Install Red Hat Enterprise Linux 7 Server on a system that has access to the Content Delivery Network. This system downloads all the required packages, and distributes them to your offline system(s).

   IMPORTANT

   Ensure that the system used in this procedure has a large amount of free disk space available. This procedure downloads a large number of packages, and requires up to 50GB of free disk space.

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

   ```
   # subscription-manager register
   ```

3. Subscribe the system to all required entitlements:

   1. Find the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscription pools and note down the pool IDs.

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

   2. Use the pool IDs located in the previous step to attach the entitlements to the system:

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

   3. Disable all existing repositories:

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

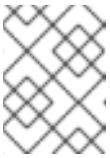
   4. Enable the required repositories:

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

   5. Ensure that all packages currently installed are up to date:

      ```
      # yum update
      ```

-



NOTE

Reboot the machine if any kernel related packages have been updated.

4. Servers that are not connected to the Internet can access software repositories on other systems using File Transfer Protocol (FTP). To create the FTP repository, install and configure vsftpd:

   a. Install the vsftpd package:

   ```
   # yum install vsftpd
   ```

   b. Start the **vsftpd** service, and ensure the service starts on boot:

   ```
   # systemctl start vsftpd.service
   # systemctl enable vsftpd.service
   ```

   c. Create a sub-directory inside the **/var/ftp/pub/** directory. This is where the downloaded packages will be made available:

   ```
   # mkdir /var/ftp/pub/rhevrepo
   ```

5. Download packages from all configured software repositories to the **rhevrepo** directory. This includes repositories for all Content Delivery Network subscription pools the system is subscribed to, and any locally configured repositories:

   ```
   # reposync -l -p /var/ftp/pub/rhevrepo
   ```

   This command downloads a large number of packages, and takes a long time to complete. The **-l** option enables yum plug-in support.

6. Install the createrepo package:

   ```
   # yum install createrepo
   ```

7. Create repository metadata for each of the sub-directories where packages were downloaded under **/var/ftp/pub/rhevrepo**:

   ```
   # for DIR in `find /var/ftp/pub/rhevrepo -maxdepth 1 -mindepth 1 -
   type d`; do createrepo $DIR; done;
   ```

8. Create a repository file, and copy it to the **/etc/yum.repos.d/** directory on the offline machine on which you will install the Manager.

   The configuration file can be created manually or with a script. Run the script below on the system hosting the repository, replacing *ADDRESS* in the ***baseurl*** with the IP address or fully qualified domain name of the system hosting the repository:

   ```
   #!/bin/sh
   ```

```
REPOFILE="/etc/yum.repos.d/rhev.repo"
echo -e " " > $REPOFILE

for DIR in `find /var/ftp/pub/rhevrepo -maxdepth 1 -mindepth 1 -type
d`;
do
    echo -e "[`basename $DIR`]" >> $REPOFILE
    echo -e "name=`basename $DIR`" >> $REPOFILE
    echo -e "baseurl=ftp://ADDRESS/pub/rhevrepo/`basename $DIR`" >>
$REPOFILE
    echo -e "enabled=1" >> $REPOFILE
    echo -e "gpgcheck=0" >> $REPOFILE
    echo -e "\n" >> $REPOFILE
done;
```

9. Install the Manager packages on the offline system. See Section 3.2, “Installing the Red Hat Virtualization Manager Packages” for instructions. Packages are installed from the local repository, instead of from the Content Delivery Network.

10. Configure the Manager. See Section 3.3, “Configuring the Red Hat Virtualization Manager” for initial configuration instructions.

11. Continue with host, storage, and virtual machine configuration.

PART III. INSTALLING HOSTS

CHAPTER 5. INTRODUCTION TO HOSTS

Red Hat Virtualization supports two types of hosts: Red Hat Virtualization Host (RHVH) and Red Hat Enterprise Linux host. Depending on your environment requirement, you may want to use one type only or both in your Red Hat Virtualization environment. It is recommended that you install and attach at least two hosts to the Red Hat Virtualization environment. Where you attach only one host you will be unable to access features such as migration and high availability.

IMPORTANT

SELinux is in enforcing mode upon installation. To verify, run **`getenforce`**. SELinux is required to be in enforcing mode on all hypervisors and Managers for your Red Hat Virtualization environment to be supported by Red Hat.

Table 5.1. Hosts

Host Type	Other Names	Description
`Red Hat Virtualization Host`	RHVH, thin host	This is a minimal operating system based on Red Hat Enterprise Linux. It is distributed as an ISO file from the Customer Portal and contains only the packages required for the machine to act as a host.
`Red Hat Enterprise Linux Host`	RHEL-based hypervisor, thick host	Red Hat Enterprise Linux hosts subscribed to the appropriate channels can be used as hosts.

5.1. HOST COMPATIBILITY

When you create a new data center, you can set the compatibility version. Select the compatibility version that suits all the hosts in the data center. Once set, version regression is not allowed. For a fresh Red Hat Virtualization installation, the latest compatibility version is set in the default data center and default cluster; to use an older compatibility version, you must create additional data centers and clusters. For more information about compatibility versions see *Red Hat Virtualization Manager Compatibility* in the Red Hat Virtualization Life Cycle.

CHAPTER 6. RED HAT VIRTUALIZATION HOSTS

Red Hat Virtualization 4.0 introduces an upgraded version of the Red Hat Enterprise Virtualization Hypervisor. While the previous RHEV-H was a closed system with a basic text user interface for installation and configuration, Red Hat Virtualization Host (RHVH) can be updated via **yum** and uses an **Anaconda** installation interface based on the one used by Red Hat Enterprise Linux hosts.

6.1. INSTALLING RED HAT VIRTUALIZATION HOST

Red Hat Virtualization Host (RHVH) is a minimal operating system based on Red Hat Enterprise Linux that is designed to provide a simple method for setting up a physical machine to act as a hypervisor in a Red Hat Virtualization environment. The minimal operating system contains only the packages required for the machine to act as a hypervisor, and features a Cockpit user interface for monitoring the host and performing administrative tasks. See http://cockpit-project.org/running.html for the minimum browser requirements.

RHVH supports NIST 800-53 partitioning requirements to improve security. RHVH uses a NIST 800-53 partition layout by default.

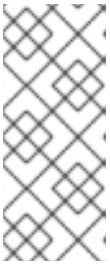
Before you proceed, make sure the machine on which you are installing RHVH meets the hardware requirements listed in Section 2.2, “Hypervisor Requirements”.

Installing RHVH on a physical machine involves three key steps:

1. Download the RHVH ISO image from the Customer Portal.
2. Write the RHVH ISO image to a USB, CD, or DVD.
3. Install the RHVH minimal operating system.

Procedure 6.1. Installing Red Hat Virtualization Host

1. Download the RHVH ISO image from the Customer Portal:
   a. Log in to the Customer Portal at https://access.redhat.com.
   b. Click **Downloads** in the menu bar.
   c. Click **Red Hat Virtualization**, scroll up, and click **Download Latest** to access the product download page.
   d. Choose the appropriate hypervisor image and click **Download Now**.
   e. Create a bootable media device. See Making Media in the *Red Hat Enterprise Linux Installation Guide* for more information.
2. Start the machine on which to install RHVH using the prepared installation media.
3. From the boot menu, select the **Install** option, and press **Enter**.



NOTE

You can also press the **Tab** key to edit the kernel parameters. Kernel parameters must be separated by a space, and you can boot the system using the specified kernel parameters by pressing the **Enter** key. Press the **Esc** key to clear any changes to the kernel parameters and return to the boot menu.

4. Select a language, and click **Continue**.
5. Select a time zone from the **Date & Time** screen and click **Done**.
6. Select a keyboard layout from the **Keyboard** screen and click **Done**.
7. Select the device on which to install RHVH from the **Installation Destination** screen. Optionally, enable encryption. Click **Done**.

IMPORTANT

Red Hat strongly recommends using the **Automatically configure partitioning** option.

NOTE

For information on preserving local storage domains when reinstalling RHVH, see Upgrading to RHVH While Preserving Local Storage in the *Upgrade Guide*.

8. Select a network from the **Network & Host Name** screen and click **Configure...** to configure the connection details. Enter a host name in the **Host name** field, and click **Done**.
9. Optionally configure **Language Support**, **Security Policy**, and **Kdump**. See Installing Using Anaconda in the *Red Hat Enterprise Linux 7 Installation Guide* for more information on each of the sections in the **Installation Summary** screen.
10. Click **Begin Installation**.
11. Set a root password and, optionally, create an additional user while RHVH installs.

WARNING

Red Hat strongly recommends not creating untrusted users on RHVH, as this can lead to exploitation of local security vulnerabilities.

12. Click **Reboot** to complete the installation.

NOTE

When RHVH restarts, **imgbase-motd.service** performs a health check on the host and displays the result when you log in on the command line. The message **imgbase status: OK** or **imgbase status: DEGRADED** indicates the health status. Run **imgbase check** to get more information. The service is enabled by default.

13. Once the installation is complete, log in to the Cockpit user interface at https://*HostFQDNorIP*:9090 to subscribe the host to the Content Delivery Network. Click **Tools** > **Subscriptions** > **Register System** and enter your Customer Portal username and password. The system automatically subscribes to the **Red Hat Virtualization Host** entitlement.

14. Click **Terminal**, and enable the **Red Hat Virtualization Host 7** repository to allow later updates to the Red Hat Virtualization Host:

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

You can now add the host to your Red Hat Virtualization environment. See Chapter 8, *Adding a Host to the Red Hat Virtualization Manager*.

WARNING

Configuring networking through NetworkManager (including **nmcli**, **nmtui**, and the Cockpit user interface) is currently not supported. If additional network configuration is required before adding a host to the Manager, you must manually write **ifcfg** files. See the *Red Hat Enterprise Linux Networking Guide* for more information.

6.2. ADVANCED INSTALLATION

6.2.1. Custom Partitioning

Custom partitioning on Red Hat Virtualization Host (RHVH) is not recommended. Red Hat strongly recommends using the **Automatically configure partitioning** option in the **Installation Destination** window.

If your installation requires custom partitioning, note that the following restrictions apply:

- You must select the **LVM Thin Provisioning** option in the **Manual Partitioning** window.
- The root (**/**) directory must be on a thinly provisioned logical volume.
- The root (**/**) directory must be at least 6 GB.
- The **/var** directory must be on a separate volume or disk.
- Only XFS or Ext4 file systems are supported.

6.2.2. Automating Red Hat Virtualization Host Deployment

You can install Red Hat Virtualization Host (RHVH) without a physical media device by booting from the network using PXE. You can automate the installation process by using a Kickstart file containing the answers to the installation questions. The Kickstart file can also be accessed over the network, removing the need for physical media.

Instructions for both tasks can be found in the Red Hat Enterprise Linux 7 *Installation Guide*, as RHVH is installed in much the same way as Red Hat Enterprise Linux. The main differences required for RHVH are included in the following procedure.

Procedure 6.2. Automating Deployment using PXE and Kickstart

1. Download the RHVH ISO image from the Customer Portal:
   a. Log in to the Customer Portal at https://access.redhat.com.
   b. Click **Downloads** in the menu bar.
   c. Click **Red Hat Virtualization**, scroll up, and click **Download Latest** to access the product download page.
   d. Choose the appropriate hypervisor image and click **Download Now**.
2. Make the RHVH ISO image available over the network using the instructions in Installation Source on a Network.
3. Configure the PXE server using the instructions in Preparing for a Network Installation.

   The following requirements apply in order to boot RHVH from the PXE server:

   - Ensure that you copy the RHVH boot images to the **tftp/** root directory.

     ```
     # cp URL/to/RHVH-ISO/images/pxeboot/{vmlinuz,initrd.img}
     /var/lib/tftpboot/pxelinux/
     ```

   - The boot loader configuration file must include a RHVH label that specifies the RHVH boot images.

     ```
     KERNEL URL/to/vmlinuz
     APPEND initrd=URL/to/initrd.img inst.stage2=URL/to/RHVH-ISO
     ```

4. Create a Kickstart file and make it available over the network using the instructions in Kickstart Installations.

   The following constraints apply to RHVH Kickstart files:

   - The **%packages** section is not required for RHVH. Instead, use the **liveimg** option and specify the **squashfs.img** file from the RHVH ISO image.

     ```
     liveimg --url=URL/to/squashfs.img
     ```

   - The **autopart** command is highly recommended. Thin provisioning must be used.

     ```
     autopart --type=thinp
     ```

If your installation requires manual partitioning instead, the following limitations apply:

- The root (/) directory must be on a thinly provisioned logical volume.
- The **/var** directory must be on a separate volume.
- The **/boot** directory must be on a separate partition.

- A **%post** section that calls the **nodectl init** command is required.

```
%post
nodectl init
%end
```

To fully automate the installation process, you can add this Kickstart file to the boot loader configuration file on the PXE server. Specify the Kickstart location by adding **inst.ks=** to the **APPEND** line:

```
APPEND initrd=URL/to/initrd.img inst.stage2=URL/to/RHVH-ISO
inst.ks=URL/to/RHVH-ks.cfg
```

Example 6.1. Red Hat Virtualization Host Kickstart File

The following is an example of a Kickstart file used to deploy Red Hat Virtualization Host. You can include additional commands and options as required.

```
liveimg --url=http://1.2.3.4/path/to/squashfs.img
clearpart --all
autopart --type=thinp
rootpw --plaintext ovirt
timezone --utc America/Phoenix
zerombr
text

reboot

%post --erroronfail
nodectl init
%end
```

5. Install RHVH using the instructions in Booting the Installation on AMD64 and Intel 64 Systems from the Network Using PXE.

CHAPTER 7. RED HAT ENTERPRISE LINUX HOSTS

7.1. INSTALLING RED HAT ENTERPRISE LINUX HOSTS

A Red Hat Enterprise Linux host, also known as a RHEL-based hypervisor is based on a standard basic installation of Red Hat Enterprise Linux on a physical server, with **Red Hat Enterprise Linux Server** and the **Red Hat Virtualization** entitlements enabled. For detailed installation instructions, see Red Hat Enterprise Linux 7 Installation Guide.

See Appendix G, *Configuring a Host for PCI Passthrough* for more information on how to enable the host hardware and software for device passthrough.

IMPORTANT

Virtualization must be enabled in your host's BIOS settings. For information on changing your host's BIOS settings, refer to your host's hardware documentation.

IMPORTANT

Third-party watchdogs should not be installed on Red Hat Enterprise Linux hosts, as they can interfere with the watchdog daemon provided by VDSM.

7.2. SUBSCRIBING TO THE REQUIRED ENTITLEMENTS

To be used as a virtualization host, make sure the Red Hat Enterprise Linux host meets the hardware requirements listed in Section 2.2, “Hypervisor Requirements”. The host must also be registered and subscribed to a number of entitlements using Subscription Manager. Follow this procedure to register with the Content Delivery Network and attach the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** entitlements to the host.

Procedure 7.1. Subscribing to Required Entitlements using Subscription Manager

1. Register your system with the Content Delivery Network, entering your Customer Portal **Username** and **Password** when prompted:

   ```
   # subscription-manager register
   ```

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

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

3. Use the pool IDs located in the previous step to attach the entitlements to the system:

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

NOTE

To find out what subscriptions are currently attached, run:

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

To list all enabled repositories, run:

```
# yum repolist
```

4. Disable all existing repositories:

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

5. Enable the required repositories:

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

If you are installing Red Hat Enterprise Linux 7 hosts, little endian on IBM POWER8 hardware, enable the following repositories instead:

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

6. Ensure that all packages currently installed are up to date:

```
# yum update
```

NOTE

Reboot the machine if any kernel related packages have been updated.

Once you have subscribed the host to the required entitlements, proceed to the next section to attach your host to your Red Hat Virtualization environment.

WARNING

Configuring networking through NetworkManager (including **nmcli** and **nmtui**) is currently not supported. If additional network configuration is required before adding a host to the Manager, you must manually write **ifcfg** files. See the *Red Hat Enterprise Linux Networking Guide* for more information.

CHAPTER 8. ADDING A HOST TO THE RED HAT VIRTUALIZATION MANAGER

Adding a host to your Red Hat Virtualization environment can take some time, as the following steps are completed by the platform: virtualization checks, installation of packages, creation of bridge, and a reboot of the host. Use the details pane to monitor the process as the host and the Manager establish a connection.

Procedure 8.1. Adding a Host to the Red Hat Virtualization Manager

1. From the Administration Portal, click the **Hosts** resource tab.
2. Click **New**.
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. Click the **Advanced Parameters** button to expand the advanced host settings.
   a. Optionally disable automatic firewall configuration.
   b. Optionally add a host SSH fingerprint to increase security. You can add it manually, or fetch it automatically.
7. 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*.
8. Click **OK**.

The new host displays in the list of hosts with a status of **Installing**, and you can view the progress of the installation in the details pane. After a brief delay the host status changes to **Up**.

PART IV. ATTACHING STORAGE

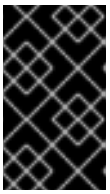
CHAPTER 9. STORAGE

9.1. INTRODUCTION TO STORAGE

A storage domain is a collection of images that have a common storage interface. A storage domain contains complete images of templates and virtual machines (including snapshots), ISO files, and metadata about themselves. A storage domain can be made of either block devices (SAN - iSCSI or FCP) or a file system (NAS - NFS, GlusterFS, or other POSIX compliant file systems).

There are three types of storage domain:

- **Data Domain:** A data domain holds the virtual hard disks and OVF files of all the virtual machines and templates in a data center, and cannot be shared across data centers. Data domains of multiple types (iSCSI, NFS, FC, POSIX, and Gluster) can be added to the same data center, provided they are all shared, rather than local, domains.



IMPORTANT

You must have one host with the status of **Up** and have attached a data domain to a data center before you can attach an ISO domain and an export domain.

- **ISO Domain:** ISO domains store ISO files (or logical CDs) used to install and boot operating systems and applications for the virtual machines, and can be shared across different data centers. An ISO domain removes the data center's need for physical media. ISO domains can only be NFS-based. Only one ISO domain can be added to a data center.

- **Export Domain:** Export domains are temporary storage repositories that are used to copy and move images between data centers and Red Hat Virtualization environments. Export domains can be used to backup virtual machines. An export domain can be moved between data centers, however, it can only be active in one data center at a time. Export domains can only be NFS-based. Only one export domain can be added to a data center.

See the next section to attach existing FCP storage as a data domain. More storage options are available in the Administration Guide

9.2. ADDING FCP STORAGE

Red Hat Virtualization platform supports SAN storage by creating a storage domain from a volume group made of pre-existing LUNs. Neither volume groups nor LUNs can be attached to more than one storage domain at a time.

Red Hat Virtualization system administrators need a working knowledge of Storage Area Networks (SAN) concepts. SAN usually uses Fibre Channel Protocol (FCP) for traffic between hosts and shared external storage. For this reason, SAN may occasionally be referred to as FCP storage.

For information regarding the setup and configuration of FCP or multipathing on Red Hat Enterprise Linux, see the Storage Administration Guide and DM Multipath Guide.

The following procedure shows you how to attach existing FCP storage to your Red Hat Virtualization environment as a data domain. For more information on other supported storage types, see Storage in the *Administration Guide*.

Procedure 9.1. Adding FCP Storage

1. Click the **Storage** resource tab to list all storage domains.
2. Click **New Domain** to open the **New Domain** window.
3. Enter the **Name** of the storage domain.

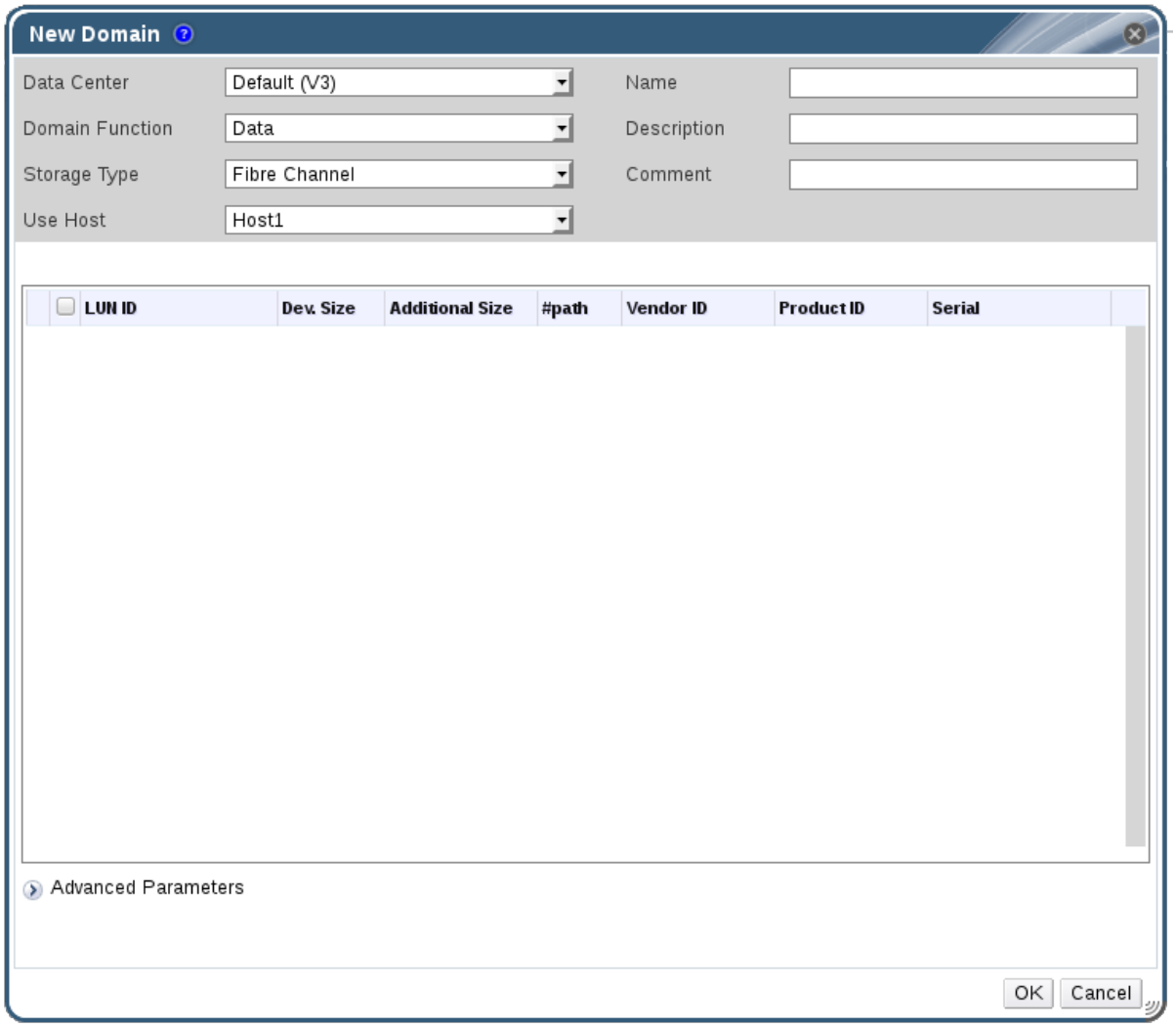


Figure 9.1. Adding FCP Storage

4. Use the **Data Center** drop-down menu to select an FCP data center.

   If you do not yet have an appropriate FCP data center, select **(none)**.

5. Use the drop-down menus to select the **Domain Function** and the **Storage Type**. The storage domain types that are not compatible with the chosen data center are not available.
6. Select an active host in the **Use Host** field. If this is not the first data domain in a data center, you must select the data center's SPM host.

IMPORTANT

All communication to the storage domain is through the selected host and not directly from the Red Hat Virtualization Manager. At least one active host must exist in the system and be attached to the chosen data center. All hosts must have access to the storage device before the storage domain can be configured.

7. The **New Domain** window automatically displays known targets with unusedLUNs when **Data / Fibre Channel** is selected as the storage type. Select the**LUN ID** check box to select all of the available LUNs.

8. Optionally, you can configure the advanced parameters.

    a. Click **Advanced Parameters**.

    b. Enter a percentage value into the **Warning Low Space Indicator** field. If the free space available on the storage domain is below this percentage, warning messages are displayed to the user and logged.

    c. Enter a GB value into the **Critical Space Action Blocker** field. If the free space available on the storage domain is below this value, error messages are displayed to the user and logged, and any new action that consumes space, even temporarily, will be blocked.

    d. Select the **Wipe After Delete** check box to enable the wipe after delete option. This option can be edited after the domain is created, but doing so will not change the wipe after delete property of disks that already exist.

9. Click **OK** to create the storage domain and close the window.

The new FCP data domain displays on the **Storage** tab. It will remain with a**Locked** status while it is being prepared for use. When ready, it is automatically attached to the data center.

APPENDIX A. CHANGING THE PERMISSIONS FOR THE LOCAL ISO DOMAIN

If the Manager was configured during setup to provide a local ISO domain, that domain can be attached to one or more data centers, and used to provide virtual machine image files. By default, the access control list (ACL) for the local ISO domain provides read and write access for only the Manager machine. Virtualization hosts require read and write access to the ISO domain in order to attach the domain to a data center. Use this procedure if network or host details were not available at the time of setup, or if you need to update the ACL at any time.

While it is possible to allow read and write access to the entire network, it is recommended that you limit access to only those hosts and subnets that require it.

Procedure A.1. Changing the Permissions for the Local ISO Domain

1. Log in to the Manager machine.
2. Edit the **/etc/exports** file, and add the hosts, or the subnets to which they belong, to the access control list:

   ```
   /var/lib/exports/iso 10.1.2.0/255.255.255.0(rw)
   host01.example.com(rw) host02.example.com(rw)
   ```

   The example above allows read and write access to a single /24 network and two specific hosts. **/var/lib/exports/iso** is the default file path for the ISO domain. See the **exports(5)** man page for further formatting options.
3. Apply the changes:

   ```
   # exportfs -ra
   ```

Note that if you manually edit the **/etc/exports** file after running **engine-setup**, running **engine-cleanup** later will not undo the changes.

APPENDIX B. ATTACHING THE LOCAL ISO DOMAIN TO A DATA CENTER

The local ISO domain, created during the Manager installation, appears in the Administration Portal as **Unattached**. To use it, attach it to a data center. The ISO domain must be of the same **Storage Type** as the data center. Each host in the data center must have read and write access to the ISO domain. In particular, ensure that the Storage Pool Manager has access.

Only one ISO domain can be attached to a data center.

Procedure B.1. Attaching the Local ISO Domain to a Data Center

1. In the Administration Portal, click the **Data Centers** resource tab and select the appropriate data center.
2. Select the **Storage** tab in the details pane to list the storage domains already attached to the data center.
3. Click **Attach ISO** to open the **Attach ISO Library** window.
4. Click the radio button for the local ISO domain.
5. Click **OK**.

The ISO domain is now attached to the data center and is automatically activated.

APPENDIX C. ENABLING GLUSTER PROCESSES ON RED HAT GLUSTER STORAGE NODES

1. In the Navigation Pane, select the **Clusters** tab.
2. Select **New**.
3. Select the "Enable Gluster Service" radio button. Provide the address, SSH fingerprint, and password as necessary. The address and password fields can be filled in only when the **Import existing Gluster configuration** check box is selected.

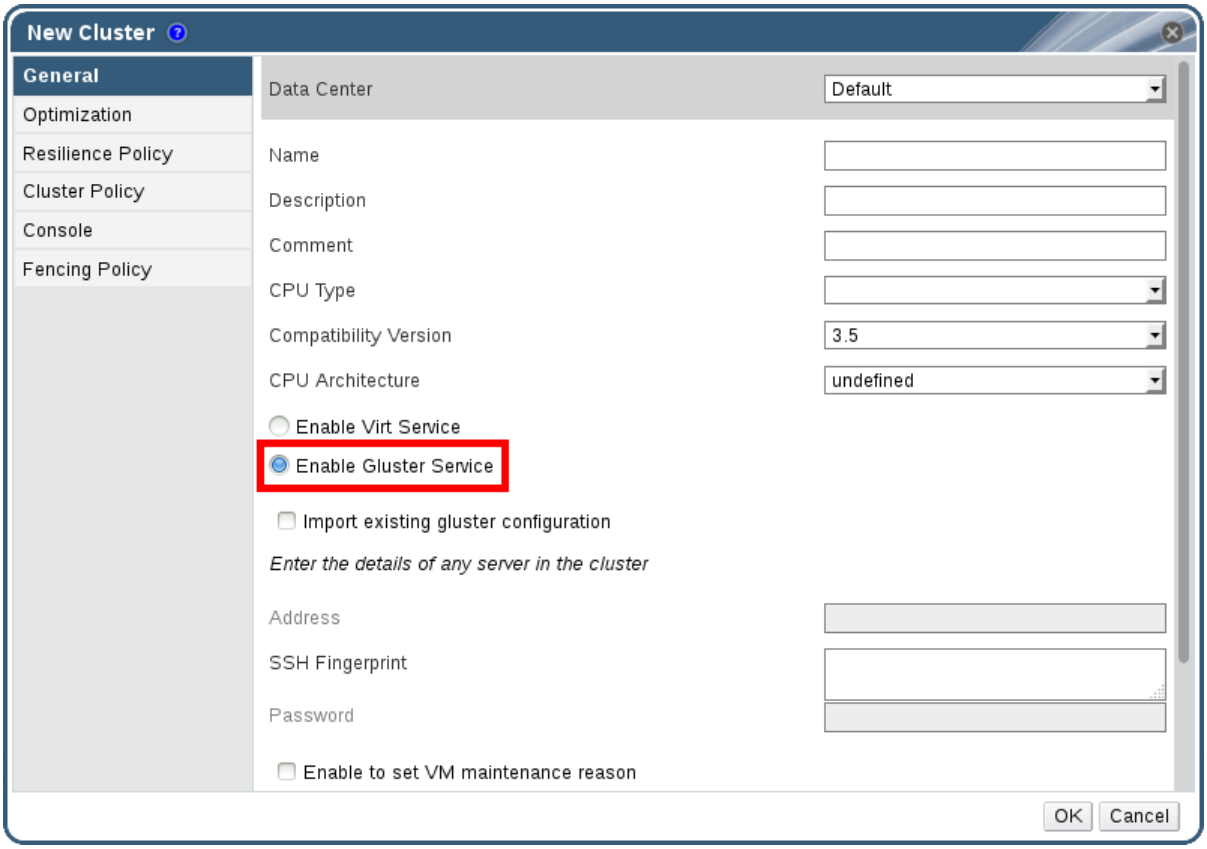


Figure C.1. Selecting the "Enable Gluster Service" Radio Button

4. Click **OK**.

It is now possible to add Red Hat Gluster Storage nodes to the Gluster cluster, and to mount Gluster volumes as storage domains. **iptables** rules no longer block storage domains from being added to the cluster.

APPENDIX D. PREPARING A REMOTE POSTGRESQL DATABASE FOR USE WITH THE RED HAT VIRTUALIZATION MANAGER

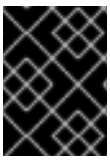
Optionally configure a PostgreSQL database on a remote Red Hat Enterprise Linux 7 machine to use as the Manager database. By default, the Red Hat Virtualization Manager's configuration script, **engine-setup**, creates and configures the Manager database locally on the Manager machine. For automatic database configuration, see Section 3.3, “Configuring the Red Hat Virtualization Manager”. To set up the Manager database with custom values on the Manager machine, see Appendix E, *Preparing a Local Manually-Configured PostgreSQL Database for Use with the Red Hat Virtualization Manager*.

Use this procedure to configure the database on a machine that is separate from the machine where the Manager is installed. Set up this database before you configure the Manager; you must supply the database credentials during **engine-setup**.

NOTE

The **engine-setup** and **engine-backup --mode=restore** commands only support system error messages in the **en_US.UTF8** locale, even if the system locale is different.

The locale settings in the **postgresql.conf** file must be set to **en_US.UTF8**.



IMPORTANT

The database name must contain only numbers, underscores, and lowercase letters.

Procedure D.1. Preparing a Remote PostgreSQL Database for use with the Red Hat Virtualization Manager

1. Install the PostgreSQL server package:

```
# yum install postgresql-server
```

2. Initialize the PostgreSQL database, start the **postgresql** service, and ensure that this service starts on boot:

```
# su -l postgres -c "/usr/bin/initdb --locale=en_US.UTF8 --
auth='ident' --pgdata=/var/lib/pgsql/data/"
# systemctl start postgresql.service
# systemctl enable postgresql.service
```

3. Connect to the **psql** command line interface as the **postgres** user:

```
# su - postgres
$ psql
```

4. Create a user for the Manager to use when it writes to and reads from the database. The default user name on the Manager is **engine**:

```
postgres=# create role user_name with login encrypted password
'password';
```

5. Create a database in which to store data about the Red Hat Virtualization environment. The default database name on the Manager is **engine**:

```
postgres=# create database database_name owner user_name template
template0 encoding 'UTF8' lc_collate 'en_US.UTF-8' lc_ctype
'en_US.UTF-8';
```

6. Connect to the new database and add the **plpgsql** language:

```
postgres=# \c database_name
database_name=# CREATE LANGUAGE plpgsql;
```

7. Ensure the database can be accessed remotely by enabling md5 client authentication. Edit the **/var/lib/pgsql/data/pg_hba.conf** file, and add the following line immediately underneath the line starting with **local** at the bottom of the file, replacing *X.X.X.X* with the IP address of the Manager:

```
host    database_name    user_name    X.X.X.X/32    md5
```

8. Allow TCP/IP connections to the database. Edit the **/var/lib/pgsql/data/postgresql.conf** file and add the following line:

```
listen_addresses='*'
```

   This example configures the **postgresql** service to listen for connections on all interfaces. You can specify an interface by giving its IP address.

9. Open the default port used for PostgreSQL database connections, and save the updated firewall rules:

```
# yum install iptables-services
# iptables -I INPUT 5 -p tcp --dport 5432 -j ACCEPT
# service iptables save
```

10. Restart the **postgresql** service:

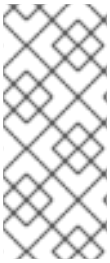
```
# systemctl restart postgresql.service
```

Optionally, set up SSL to secure database connections using the instructions at http://www.postgresql.org/docs/9.2/static/ssl-tcp.html#SSL-FILE-USAGE.

APPENDIX E. PREPARING A LOCAL MANUALLY-CONFIGURED POSTGRESQL DATABASE FOR USE WITH THE RED HAT VIRTUALIZATION MANAGER

Optionally configure a local PostgreSQL database on the Manager machine to use as the Manager database. By default, the Red Hat Virtualization Manager's configuration script, **engine-setup**, creates and configures the Manager database locally on the Manager machine. For automatic database configuration, see Section 3.3, “Configuring the Red Hat Virtualization Manager”. To configure the Manager database on a machine that is separate from the machine where the Manager is installed, see Appendix D, *Preparing a Remote PostgreSQL Database for Use with the Red Hat Virtualization Manager*.

Use this procedure to set up the Manager database with custom values. Set up this database before you configure the Manager; you must supply the database credentials during **engine-setup**. To set up the database, you must first install the rhevm package on the Manager machine; the postgresql-server package is installed as a dependency.



NOTE

The **engine-setup** and **engine-backup --mode=restore** commands only support system error messages in the **en_US.UTF8** locale, even if the system locale is different.

The locale settings in the **postgresql.conf** file must be set to **en_US.UTF8**.

IMPORTANT

The database name must contain only numbers, underscores, and lowercase letters.

Procedure E.1. Preparing a Local Manually-Configured PostgreSQL Database for use with the Red Hat Virtualization Manager

1. Initialize the PostgreSQL database, start the **postgresql** service, and ensure that this service starts on boot:

```
# su -l postgres -c "/usr/bin/initdb --locale=en_US.UTF8 --
auth='ident' --pgdata=/var/lib/pgsql/data/"
# systemctl start postgresql.service
# systemctl enable postgresql.service
```

2. Connect to the **psql** command line interface as the **postgres** user:

```
# su - postgres
$ psql
```

3. Create a user for the Manager to use when it writes to and reads from the database. The default user name on the Manager is **engine**:

```
postgres=# create role user_name with login encrypted password
'password';
```

4. Create a database in which to store data about the Red Hat Virtualization environment. The default database name on the Manager is **engine**:

```
postgres=# create database database_name owner user_name template
template0 encoding 'UTF8' lc_collate 'en_US.UTF-8' lc_ctype
'en_US.UTF-8';
```

5. Connect to the new database and add the **plpgsql** language:

```
postgres=# \c database_name
database_name=# CREATE LANGUAGE plpgsql;
```

6. Ensure the database can be accessed remotely by enabling md5 client authentication. Edit the **/var/lib/pgsql/data/pg_hba.conf** file, and add the following line immediately underneath the line starting with **local** at the bottom of the file:

```
host    [database name]    [user name]    0.0.0.0/0  md5
host    [database name]    [user name]    ::0/0      md5
```

7. Restart the **postgresql** service:

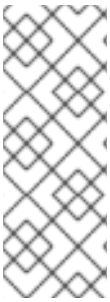
```
# systemctl restart postgresql.service
```

Optionally, set up SSL to secure database connections using the instructions at http://www.postgresql.org/docs/8.4/static/ssl-tcp.html#SSL-FILE-USAGE.

APPENDIX F. INSTALLING A WEBSOCKET PROXY ON A SEPARATE MACHINE

The websocket proxy allows users to connect to virtual machines via noVNC and SPICE HTML5 consoles. The noVNC client uses websockets to pass VNC data. However, the VNC server in QEMU does not provide websocket support, therefore a websocket proxy must be placed between the client and the VNC server. The proxy can run on any machine that has access to the network, including the the Manager machine.

For security and performance reasons, users may want to configure the websocket proxy on a separate machine.



NOTE

SPICE HTML5 support is a Technology Preview feature. Technology Preview features are not fully supported under Red Hat Subscription Service Level Agreements (SLAs), may not be functionally complete, and are not intended for production use. However, these features provide early access to upcoming product innovations, enabling customers to test functionality and provide feedback during the development process.

This section describes how to install and configure the websocket proxy on a separate machine that does not run the Manager. See Section 3.3, “Configuring the Red Hat Virtualization Manager” for instructions on how to configure the websocket proxy on the Manager.

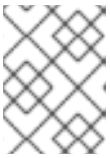
Procedure F.1. Installing and Configuring a Websocket Proxy on a Separate Machine

1. Install the websocket proxy:

```
# yum install ovirt-engine-websocket-proxy
```

2. Run the **engine-setup** command to configure the websocket proxy.

```
# engine-setup
```



NOTE

If the rhevm package has also been installed, choose **No** when asked to configure the engine on this host.

3. Press **Enter** to allow **engine-setup** to configure a websocket proxy server on the machine.

```
Configure WebSocket Proxy on this machine? (Yes, No) [Yes]:
```

4. Press **Enter** to accept the automatically detected hostname, or enter an alternative hostname and press **Enter**. Note that the automatically detected hostname may be incorrect if you are using virtual hosts:

```
Host fully qualified DNS name of this server [host.example.com]:
```

5. Press **Enter** to allow **engine-setup** to configure the firewall and open the ports required for external communication. If you do not allow **engine-setup** to modify your firewall configuration, then you must manually open the required ports.

```
Setup can automatically configure the firewall on this system.
Note: automatic configuration of the firewall may overwrite current
settings.
Do you want Setup to configure the firewall? (Yes, No) [Yes]:
```

6. Enter the fully qualified DNS name of the Manager machine and press **Enter**.

```
Host fully qualified DNS name of the engine server []:
engine_host.example.com
```

7. Press **Enter** to allow **engine-setup** to perform actions on the Manager machine, or press **2** to manually perform the actions.

```
Setup will need to do some actions on the remote engine server.
Either automatically, using ssh as root to access it, or you will be
prompted to manually perform each such action.
Please choose one of the following:
1 - Access remote engine server using ssh as root
2 - Perform each action manually, use files to copy content around
(1, 2) [1]:
```

   a. Press **Enter** to accept the default SSH port number, or enter the port number of the Manager machine.

```
ssh port on remote engine server [22]:
```

   b. Enter the root password to log in to the Manager machine and press **Enter**.

```
root password on remote engine server engine_host.example.com:
```

8. Select whether to review iptables rules if they differ from the current settings.

```
Generated iptables rules are different from current ones.
Do you want to review them? (Yes, No) [No]:
```

9. Press **Enter** to confirm the configuration settings.

```
--== CONFIGURATION PREVIEW ==--

Firewall manager                        : iptables
Update Firewall                         : True
Host FQDN                               : host.example.com
Configure WebSocket Proxy               : True
Engine Host FQDN                        : engine_host.example.com

Please confirm installation settings (OK, Cancel) [OK]:
```

Instructions are provided to configure the Manager machine to use the configured websocket proxy.

```
Manual actions are required on the engine host
in order to enroll certs for this host and configure the engine
about it.

Please execute this command on the engine host:
   engine-config -s WebSocketProxy=host.example.com:6100
and than restart the engine service to make it effective
```

10. Log in to the Manager machine and execute the provided instructions.

```
# engine-config -s WebSocketProxy=host.example.com:6100
# systemctl restart ovirt-engine.service
```

APPENDIX G. CONFIGURING A HOST FOR PCI PASSTHROUGH

Enabling PCI passthrough allows a virtual machine to use a host device as if the device were directly attached to the virtual machine. To enable the PCI passthrough function, you need to enable virtualization extensions and the IOMMU function. The following procedure requires you to reboot the host. If the host is attached to the Manager already, ensure you place the host into maintenance mode before running the following procedure.

Prerequisites:

- Ensure that the host hardware meets the requirements for PCI device passthrough and assignment. See Section 2.2.4, “PCI Device Requirements” for more information.

Procedure G.1. Configuring a Host for PCI Passthrough

1. Enable the virtualization extension and IOMMU extension in the BIOS. See Enabling Intel VT-x and AMD-V virtualization hardware extensions in BIOS in the *Red Hat Enterprise Linux Virtualization and Administration Guide* for more information.

2. Enable the IOMMU flag in the kernel by selecting the **Hostdev Passthrough & SR-IOV** check box when adding the host to the Manager or by editing the **grub** configuration file manually.

   - To enable the IOMMU flag from the Administration Portal, see Adding a Host to the Red Hat Virtualization Manager and Kernel Settings Explained in the *Administration Guide*.

   - To edit the **grub** configuration file manually, see Procedure G.2, “Enabling IOMMU Manually”.

3. For GPU passthrough, you need to run additional configuration steps on both the host and the guest system. See Preparing Host and Guest Systems for GPU Passthrough in the *Administration Guide* for more information.

Procedure G.2. Enabling IOMMU Manually

1. Enable IOMMU by editing the grub configuration file.

   NOTE

   If you are using IBM POWER8 hardware, skip this step as IOMMU is enabled by default.

   - For Intel, boot the machine, and append **intel_iommu=on** to the end of the **GRUB_CMDLINE_LINUX** line in the **grub** configuration file.

     ```
     # vi /etc/default/grub
     ...
     GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ...
     intel_iommu=on
     ...
     ```

- For AMD, boot the machine, and append **amd_iommu=on** to the end of the **GRUB_CMDLINE_LINUX** line in the **grub** configuration file.

```
# vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ...
amd_iommu=on
...
```

NOTE

If **intel_iommu=on** or **amd_iommu=on** works, you can try replacing them with **iommu=pt** or **amd_iommu=pt**. The **pt** option only enables IOMMU for devices used in passthrough and will provide better host performance. However, the option may not be supported on all hardware. Revert to previous option if the **pt** option doesn't work for your host.

If the passthrough fails because the hardware does not support interrupt remapping, you can consider enabling the **allow_unsafe_interrupts** option if the virtual machines are trusted. The **allow_unsafe_interrupts** is not enabled by default because enabling it potentially exposes the host to MSI attacks from virtual machines. To enable the option:

```
# vi /etc/modprobe.d
options vfio_iommu_type1 allow_unsafe_interrupts=1
```

2. Refresh the **grub.cfg** file and reboot the host for these changes to take effect:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

```
# reboot
```

For enabling SR-IOV and assigning dedicated virtual NICs to virtual machines, see https://access.redhat.com/articles/2335291 for more information.