Red Hat Virtualization 4.4

Installing Red Hat Virtualization as a standalone Manager with remote databases

Installing the Red Hat Virtualization Manager on one server, and its databases on a second server

Last Updated: 2024-02-26

Red Hat Virtualization 4.4 Installing Red Hat Virtualization as a standalone Manager with remote databases

Installing the Red Hat Virtualization Manager on one server, and its databases on a second server

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

Legal Notice

Abstract

This document describes how to install a standalone Manager environment – where the Red Hat Virtualization Manager is installed on either a physical server or a virtual machine hosted in another environment – with the Manager database and the Data Warehouse service and database hosted on a remote server. Although you can choose to host one database locally and the other remotely, this document assumes that both databases will be hosted remotely. If this is not the configuration you want to use, see the other Installation Options in the Product Guide.

Table of Contents

PREFACE

Standalone Manager installation is manual and customizable. You must install a Red Hat Enterprise Linux machine, then run the configuration script (**engine-setup**) and provide information about how you want to configure the Red Hat Virtualization Manager. Add hosts and storage after the Manager is running. At least two hosts are required for virtual machine high availability.

To install the Manager with a remote Manager database, manually create the database on the remote machine before running **engine-setup**. To install the Data Warehouse database on a remote machine, run the Data Warehouse configuration script (**ovirt-engine-dwh-setup**) on the remote machine. This script installs the Data Warehouse service and can create the Data Warehouse database automatically.

See the *Planning and Prerequisites Guide* for information on environment options and recommended configuration.

RED HAT VIRTUALIZATION KEY COMPONENTS

Component Name	Description
Red Hat Virtualization Manager	A service that provides a graphical user interface and a REST API to manage the resources in the environment. The Manager is installed on a physical or virtual machine running Red Hat Enterprise Linux.
Hosts	Red Hat Enterprise Linux hosts (RHEL hosts) and Red Hat Virtualization Hosts (image-based hypervisors) are the two supported types of host. Hosts use Kernel-based Virtual Machine (KVM) technology and provide resources used to run virtual machines.
Shared Storage	A storage service is used to store the data associated with virtual machines.
Data Warehouse	A service that collects configuration information and statistical data from the Manager.

STANDALONE MANAGER ARCHITECTURE

The Red Hat Virtualization Manager runs on a physical server, or a virtual machine hosted in a separate virtualization environment. A standalone Manager is easier to deploy and manage, but requires an additional physical server. The Manager is only highly available when managed externally with a product such as Red Hat’s High Availability Add-On.

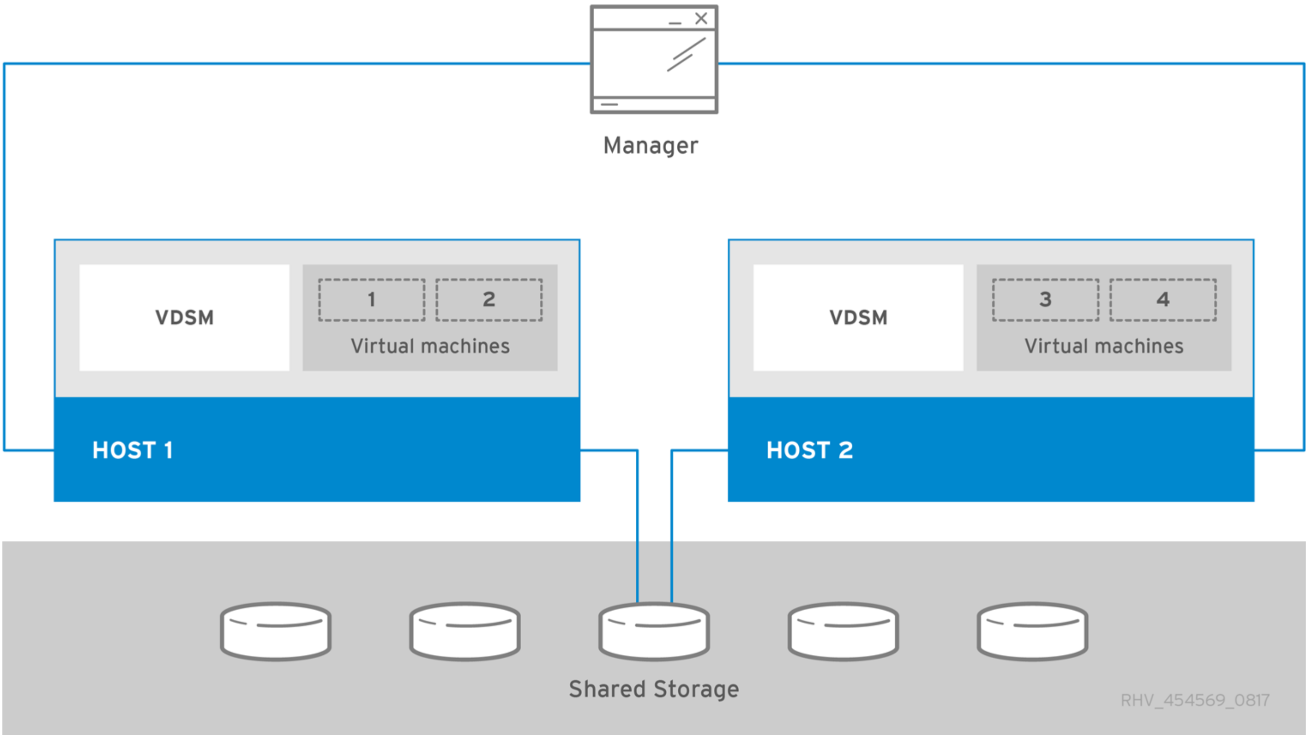
The minimum setup for a standalone Manager environment includes:

- One Red Hat Virtualization Manager machine. The Manager is typically deployed on a physical server. However, it can also be deployed on a virtual machine, as long as that virtual machine is hosted in a separate environment. The Manager must run on Red Hat Enterprise Linux 8.

- A minimum of two hosts for virtual machine high availability. You can use Red Hat Enterprise Linux hosts or Red Hat Virtualization Hosts (RHVH). VDSM (the host agent) runs on all hosts to facilitate communication with the Red Hat Virtualization Manager.

- One storage service, which can be hosted locally or on a remote server, depending on the storage type used. The storage service must be accessible to all hosts.

Figure 1. Standalone Manager Red Hat Virtualization Architecture



CHAPTER 1. INSTALLATION OVERVIEW

Installing a standalone Manager environment with remote databases involves the following steps:

1. Install and configure the Red Hat Virtualization Manager:

    a. Install two Red Hat Enterprise Linux machines: one for the Manager, and one for the databases. The second machine will be referred to as the remote server.

    b. Register the Manager machine with the Content Delivery Network and enable the Red Hat Virtualization Manager repositories.

    c. Manually configure the Manager database on the remote server. You can also use this procedure to manually configure the Data Warehouse database if you do not want the Data Warehouse setup script to configure it automatically.

    d. Configure the Red Hat Virtualization Manager using **engine-setup**.

    e. Install the Data Warehouse service and database on the remote server.

    f. Connect to the Administration Portal to add hosts and storage domains.

2. Install hosts to run virtual machines on:

    a. Use either host type, or both:

    - Red Hat Virtualization Host
    - Red Hat Enterprise Linux

    b. Add the hosts to the Manager.

3. Prepare storage to use for storage domains. You can use one of the following storage types:

    - NFS
    - iSCSI
    - Fibre Channel (FCP)
    - POSIX-compliant file system
    - Local storage
    - Red Hat Gluster Storage

4. Add storage domains to the Manager.

IMPORTANT

Keep the environment up to date. See How do I update my Red Hat Virtualization system? for more information. Since bug fixes for known issues are frequently released, use scheduled tasks to update the hosts and the Manager.

CHAPTER 2. REQUIREMENTS

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.

Hardware certification for Red Hat Virtualization is covered by the hardware certification for Red Hat Enterprise Linux. For more information, see Does Red Hat Virtualization also have hardware certification?. To confirm whether specific hardware items are certified for use with Red Hat Enterprise Linux, see Red Hat certified hardware .

Table 2.1. Red Hat Virtualization Manager Hardware Requirements

Resource	Minimum	Recommended
CPU	A dual core x86_64 CPU.	A quad core x86_64 CPU or multiple dual core x86_64 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 RHV Manager History Database Size Calculator to calculate the appropriate disk space 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 VM 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
Tier 1	Red Hat Enterprise Linux	Mozilla Firefox Extended Support Release (ESR) version
	Any	Most recent version of Google Chrome, Mozilla Firefox, or Microsoft Edge
Tier 2		
Tier 3	Any	Earlier versions of Google Chrome or Mozilla Firefox
	Any	Other browsers

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 Supporting Components on Client Machines in the *Virtual Machine Management Guide*. Installing **virt-viewer** requires Administrator privileges.

You can access virtual machine consoles using the SPICE, VNC, or RDP (Windows only) protocols. You can install the QXLDOD graphical driver in the guest operating system to improve the functionality of SPICE. SPICE currently supports a maximum resolution of 2560x1600 pixels.

Client Operating System SPICE Support

Supported QXLDOD drivers are available on Red Hat Enterprise Linux 7.2 and later, and Windows 10.

NOTE

SPICE may work with Windows 8 or 8.1 using QXLDOD drivers, but it is neither certified nor tested.

2.1.4. Operating System Requirements

The Red Hat Virtualization Manager must be installed on a base installation of Red Hat Enterprise Linux 8.6.

Do not install any additional packages after the base installation, as they may cause dependency issues when attempting to install the packages required by the Manager.

Do not enable additional repositories other than those required for the Manager installation.

2.2. HOST REQUIREMENTS

Hardware certification for Red Hat Virtualization is covered by the hardware certification for Red Hat Enterprise Linux. For more information, see Does Red Hat Virtualization also have hardware certification?. To confirm whether specific hardware items are certified for use with Red Hat Enterprise Linux, see Find a certified solution .

For more information on the requirements and limitations that apply to guests see Red Hat Enterprise Linux Technology Capabilities and Limits and Supported Limits for Red Hat Virtualization .

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.

The following CPU models are supported:

- AMD
  - Opteron G4
  - Opteron G5
  - EPYC
- Intel
  - Nehalem
  - Westmere
  - SandyBridge
  - IvyBridge
  - Haswell
  - Broadwell
  - Skylake Client
  - Skylake Server
  - Cascadelake Server
- IBM
  - POWER8
  - POWER9

For each CPU model with security updates, the **CPU Type** lists a basic type and a secure type. For example:

- **Intel Cascadelake Server Family**
- **Secure Intel Cascadelake Server Family**

The Secure CPU type contains the latest updates. For details, see BZ#1731395

2.2.1.1. 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.

Procedure

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 parameter **rescue**.
4. Press **Enter** to boot into rescue mode.
5. At the prompt, 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, the processor is hardware virtualization capable. If no output is shown, your processor may still support 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 minimum required RAM is 2 GB. For cluster levels 4.2 to 4.5, the maximum supported RAM per VM in Red Hat Virtualization Host is 6 TB. For cluster levels 4.6 to 4.7, the maximum supported RAM per VM in Red Hat Virtualization Host is 16 TB.

However, the amount of RAM required varies depending on guest operating system requirements, guest application requirements, and guest memory activity and usage. KVM can also overcommit physical RAM for virtualized guests, allowing you to provision guests with RAM requirements greater than what is physically present, on the assumption that the guests are not all working concurrently at peak load. KVM does this by only allocating RAM for guests as required and shifting underutilized guests into swap.

2.2.3. Storage Requirements

Hosts require storage to store configuration, logs, kernel dumps, and for use as swap space. Storage can be local or network-based. Red Hat Virtualization Host (RHVH) can boot with one, some, or all of its default allocations in network storage. Booting from network storage can result in a freeze if there is a network disconnect. Adding a drop-in multipath configuration file can help address losses in network connectivity. If RHVH boots from SAN storage and loses connectivity, the files become read-only until network connectivity restores. Using network storage might result in a performance downgrade.

The minimum storage requirements of RHVH 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 RHVH.

The minimum storage requirements for host installation are listed below. However, use the default allocations, which use more storage space.

- / (root) - 6 GB
- /home - 1 GB
- /tmp - 1 GB
- /boot - 1 GB
- /var - 5 GB
- /var/crash - 10 GB
- /var/log - 8 GB
- /var/log/audit - 2 GB
- /var/tmp - 10 GB
- swap - 1 GB. See What is the recommended swap size for Red Hat platforms? for details.
- Anaconda reserves 20% of the thin pool size within the volume group for future metadata expansion. This is to prevent an out-of-the-box configuration from running out of space under normal usage conditions. Overprovisioning of thin pools during installation is also not supported.
- **Minimum Total - 64 GiB**

If you are also installing the RHV-M Appliance for self-hosted engine installation, **/var/tmp** must be at least 10 GB.

If you plan to use memory overcommitment, add enough swap space to provide virtual memory for all of virtual machines. See Memory Optimization.

2.2.4. PCI Device Requirements

Hosts must have at least one network interface with a minimum bandwidth of 1 Gbps. Each host should have two network interfaces, with one dedicated to supporting network-intensive activities, such as virtual machine migration. The performance of such operations is limited by the bandwidth available.

For information about how to use PCI Express and conventional PCI devices with Intel Q35-based virtual machines, see *Using PCI Express and Conventional PCI Devices with the Q35 Virtual Machine* .

2.2.5. Device Assignment Requirements

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 devices must support ACS or ACS-equivalent capability.

- 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 8 supports PCI device assignment of PCIe-based 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.

Check vendor specification and datasheets to confirm that your hardware meets these requirements. The **lspci -v** command can be used to print information for PCI devices already installed on a system.

2.2.6. vGPU Requirements

A host must meet the following requirements in order for virtual machines on that host to use a vGPU:

- vGPU-compatible GPU

- GPU-enabled host kernel

- Installed GPU with correct drivers

- Select a vGPU type and the number of instances that you would like to use with this virtual machine using the **Manage vGPU** dialog in the **Administration Portal Host Devices** tab of the virtual machine.

- vGPU-capable drivers installed on each host in the cluster

- vGPU-supported virtual machine operating system with vGPU drivers installed

2.3. NETWORKING REQUIREMENTS

2.3.1. General requirements

Red Hat Virtualization requires IPv6 to remain enabled on the physical or virtual machine running the Manager. Do not disable IPv6 on the Manager machine, even if your systems do not use it.

2.3.2. Firewall Requirements for DNS, NTP, and IPMI Fencing

The firewall requirements for all of the following topics are special cases that require individual consideration.

DNS and NTP

Red Hat Virtualization does not create a DNS or NTP server, so the firewall does not need to have open ports for incoming traffic.

By default, Red Hat Enterprise Linux allows outbound traffic to DNS and NTP on any destination address. If you disable outgoing traffic, define exceptions for requests that are sent to DNS and NTP servers.

IMPORTANT

- The Red Hat Virtualization Manager and all hosts (Red Hat Virtualization Host and Red Hat Enterprise Linux host) must have a fully qualified domain name and full, perfectly-aligned forward and reverse name resolution.
- Running a DNS service as a virtual machine in the Red Hat Virtualization environment is not supported. All DNS services the Red Hat Virtualization environment uses must be hosted outside of the environment.
- Use DNS instead of the **/etc/hosts** file for name resolution. Using a hosts file typically requires more work and has a greater chance for errors.

IPMI and Other Fencing Mechanisms (optional)

For IPMI (Intelligent Platform Management Interface) and other fencing mechanisms, the firewall does not need to have open ports for incoming traffic.

By default, Red Hat Enterprise Linux allows outbound IPMI traffic to ports on any destination address. If you disable outgoing traffic, make exceptions for requests being sent to your IPMI or fencing servers.

Each Red Hat Virtualization Host and Red Hat Enterprise Linux host in the cluster must be able to connect to the fencing devices of all other hosts in the cluster. If the cluster hosts are experiencing an error (network error, storage error…) and cannot function as hosts, they must be able to connect to other hosts in the data center.

The specific port number depends on the type of the fence agent you are using and how it is configured.

The firewall requirement tables in the following sections do not represent this option.

2.3.3. 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.

The firewall configuration documented here assumes a default configuration.

NOTE

A diagram of these firewall requirements is available at https://access.redhat.com/articles/3932211. You can use the IDs in the table to look up connections in the diagram.

Table 2.3. Red Hat Virtualization Manager Firewall Requirements

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
M1	-	ICMP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Red Hat Virtualization Manager	Optional. May help in diagnosis.	No
M2	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.	Yes
M3	2222	TCP	Clients accessing virtual machine serial consoles.	Red Hat Virtualization Manager	Secure Shell (SSH) access to enable connection to virtual machine serial consoles.	Yes
M4	80, 443	TCP	Administration Portal clients VM Portal clients Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts REST API clients	Red Hat Virtualization Manager	Provides HTTP (port 80, not encrypted) and HTTPS (port 443, encrypted) access to the Manager. HTTP redirects connections to HTTPS.	Yes

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
M5	6100	TCP	Administration Portal clients VM Portal clients	Red Hat Virtualization Manager	Provides websocket proxy access for a web-based console client, **noVNC**, when the websocket proxy is running on the Manager.	No
M6	7410	UDP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Red Hat Virtualization Manager	If Kdump is enabled on the hosts, open this port for the fence_kdump listener on the Manager. See fence_kdump Advanced Configuration. **fence_kdump** doesn't provide a way to encrypt the connection. However, you can manually configure this port to block access from hosts that are not eligible.	No
M7	54323	TCP	Administration Portal clients	Red Hat Virtualization Manager (**ovirt-imageio** service)	Required for communication with the **ovirt-imageo** service.	Yes

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
M8	6642	TCP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Open Virtual Network (OVN) southbound database	Connect to Open Virtual Network (OVN) database	Yes
M9	9696	TCP	Clients of external network provider for OVN	External network provider for OVN	OpenStack Networking API	Yes, with configuration generated by engine-setup.
M10	35357	TCP	Clients of external network provider for OVN	External network provider for OVN	OpenStack Identity API	Yes, with configuration generated by engine-setup.
M11	53	TCP, UDP	Red Hat Virtualization Manager	DNS Server	DNS lookup requests from ports above 1023 to port 53, and responses. Open by default.	No
M12	123	UDP	Red Hat Virtualization Manager	NTP Server	NTP requests from ports above 1023 to port 123, and responses. Open by default.	No

NOTE

- A port for the OVN northbound database (6641) is not listed because, in the default configuration, the only client for the OVN northbound database (6641) is **ovirt-provider-ovn**. Because they both run on the same host, their communication is not visible to the network.
- By default, Red Hat Enterprise Linux allows outbound traffic to DNS and NTP on any destination address. If you disable outgoing traffic, make exceptions for the Manager to send requests to DNS and NTP servers. Other nodes may also require DNS and NTP. In that case, consult the requirements for those nodes and configure the firewall accordingly.

2.3.4. Host 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. The firewall rules are automatically configured by default when adding a new host to the Manager, overwriting any pre-existing firewall configuration.

To disable automatic firewall configuration when adding a new host, clear the **Automatically configure host firewall** check box under **Advanced Parameters**.

To customize the host firewall rules, see RHV: How to customize the Host's firewall rules? .

NOTE

A diagram of these firewall requirements is available at Red Hat Virtualization: Firewall Requirements Diagram. You can use the IDs in the table to look up connections in the diagram.

Table 2.4. Virtualization Host Firewall Requirements

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
H1	22	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Secure Shell (SSH) access. Optional.	Yes
H2	2223	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Secure Shell (SSH) access to enable connection to virtual machine serial consoles.	Yes

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
H3	161	UDP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	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.	No
H4	111	TCP	NFS storage server	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	NFS connections. Optional.	No
H5	5900 - 6923	TCP	Administration Portal clients VM Portal clients	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Remote guest console access via VNC and SPICE. These ports must be open to facilitate client access to virtual machines.	Yes (optional)

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
H6	5989	TCP, UDP	Common Information Model Object Manager (CIMOM)	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	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.	No
H7	9090	TCP	Red Hat Virtualization Manager Client machines	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Required to access the Cockpit web interface, if installed.	Yes
H8	16514	TCP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Virtual machine migration using **libvirt**.	Yes

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
H9	49152 - 49215	TCP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Virtual machine migration and fencing using VDSM. These ports must be open to facilitate both automated and manual migration of virtual machines.	Yes. Depending on agent for fencing, migration is done through libvirt.
H10	54321	TCP	Red Hat Virtualization Manager Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	VDSM communications with the Manager and other virtualization hosts.	Yes
H11	54322	TCP	Red Hat Virtualization Manager **ovirt-imageio** service	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Required for communication with the **ovirt-imageo** service.	Yes
H12	6081	UDP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Required, when Open Virtual Network (OVN) is used as a network provider, to allow OVN to create tunnels between hosts.	No

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
H13	53	TCP, UDP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	DNS Server	DNS lookup requests from ports above 1023 to port 53, and responses. This port is required and open by default.	No
H14	123	UDP	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	NTP Server	NTP requests from ports above 1023 to port 123, and responses. This port is required and open by default.	
H15	4500	TCP, UDP	Red Hat Virtualization Hosts	Red Hat Virtualization Hosts	Internet Security Protocol (IPSec)	Yes
H16	500	UDP	Red Hat Virtualization Hosts	Red Hat Virtualization Hosts	Internet Security Protocol (IPSec)	Yes
H17	-	AH, ESP	Red Hat Virtualization Hosts	Red Hat Virtualization Hosts	Internet Security Protocol (IPSec)	Yes

NOTE

By default, Red Hat Enterprise Linux allows outbound traffic to DNS and NTP on any destination address. If you disable outgoing traffic, make exceptions for the Red Hat Virtualization Hosts

Red Hat Enterprise Linux hosts to send requests to DNS and NTP servers. Other nodes may also require DNS and NTP. In that case, consult the requirements for those nodes and configure the firewall accordingly.

2.3.5. Database Server Firewall Requirements

Red Hat Virtualization supports the use of a remote database server for the Manager database (**engine**) and the Data Warehouse database (**ovirt-engine-history**). If you plan to use a remote database server, it must allow connections from the Manager and the Data Warehouse service (which can be separate from the Manager).

Similarly, if you plan to access a local or remote Data Warehouse database from an external system, the database must allow connections from that system.

IMPORTANT

Accessing the Manager database from external systems is not supported.

NOTE

A diagram of these firewall requirements is available at https://access.redhat.com/articles/3932211. You can use the IDs in the table to look up connections in the diagram.

Table 2.5. Database Server Firewall Requirements

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
D1	5432	TCP, UDP	Red Hat Virtualization Manager Data Warehouse service	Manager (**engine**) database server Data Warehouse (**ovirt-engine-history**) database server	Default port for PostgreSQL database connections.	No, but can be enabled.
D2	5432	TCP, UDP	External systems	Data Warehouse (**ovirt-engine-history**) database server	Default port for PostgreSQL database connections.	Disabled by default. No, but can be enabled.

2.3.6. Maximum Transmission Unit Requirements

The recommended Maximum Transmission Units (MTU) setting for Hosts during deployment is 1500. It is possible to update this setting after the environment is set up to a different MTU. For more information on changing the MTU setting, see How to change the Hosted Engine VM network MTU .

CHAPTER 3. INSTALLING THE RED HAT VIRTUALIZATION MANAGER

3.1. INSTALLING THE RED HAT VIRTUALIZATION MANAGER MACHINE AND THE REMOTE SERVER

1. The Red Hat Virtualization Manager must run on Red Hat Enterprise Linux 8. For detailed installation instructions, see *Performing a standard RHEL installation* .
   This machine must meet the minimum Manager hardware requirements.

2. Install a second Red Hat Enterprise Linux machine to use for the databases. This machine will be referred to as the remote server.

To install the Red Hat Virtualization Manager on a system that does not have access to the Content Delivery Network, see Configuring an Offline Repository for Installation before configuring the Manager.

3.2. ENABLING THE RED HAT VIRTUALIZATION MANAGER REPOSITORIES

You need to log in and register the Manager machine with Red Hat Subscription Manager, attach the **Red Hat Virtualization Manager** subscription, 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
   ```

   NOTE

   If you are using an IPv6 network, use an IPv6 transition mechanism to access the Content Delivery Network and subscription manager.

2. Find the **Red Hat Virtualization Manager** subscription pool and record the pool ID:

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

3. Use the pool ID to attach the subscription to the system:

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

NOTE

To view currently attached subscriptions:

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

To list all enabled repositories:

```
# dnf repolist
```

4. Configure the repositories:

   ```
   # subscription-manager repos \
       --disable='*' \
       --enable=rhel-8-for-x86_64-baseos-eus-rpms \
       --enable=rhel-8-for-x86_64-appstream-eus-rpms \
       --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
       --enable=fast-datapath-for-rhel-8-x86_64-rpms \
       --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
       --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
       --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
       --enable=rhel-8-for-x86_64-appstream-tus-rpms \
       --enable=rhel-8-for-x86_64-baseos-tus-rpms
   ```

5. Set the RHEL version to 8.6:

   ```
   # subscription-manager release --set=8.6
   ```

6. Enable the **pki-deps** module.

   ```
   # dnf module -y enable pki-deps
   ```

7. Enable version 12 of the **postgresql** module.

   ```
   # dnf module -y enable postgresql:12
   ```

8. Enable version 14 of the **nodejs** module:

   ```
   # dnf module -y enable nodejs:14
   ```

9. Synchronize installed packages to update them to the latest available versions.

   ```
   # dnf distro-sync --nobest
   ```

Additional resources

For information on modules and module streams, see the following sections in *Installing, managing, and removing user-space components*

- Module streams
- Selecting a stream before installation of packages

- Resetting module streams
- Switching to a later stream

Before configuring the Red Hat Virtualization Manager, you must manually configure the Manager database on the remote server. You can also use this procedure to manually configure the Data Warehouse database if you do not want the Data Warehouse setup script to configure it automatically.

3.3. PREPARING A REMOTE POSTGRESQL DATABASE

In a remote database environment, you must create the Manager database manually before running **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.

Enabling the Red Hat Virtualization Manager Repositories

You need to log in and register the database machine with Red Hat Subscription Manager, attach the **Red Hat Virtualization Manager** subscription, 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
```

NOTE

If you are using an IPv6 network, use an IPv6 transition mechanism to access the Content Delivery Network and subscription manager.

2. Find the **Red Hat Virtualization Manager** subscription pool and record the pool ID:

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

3. Use the pool ID to attach the subscription to the system:

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

NOTE

To view currently attached subscriptions:

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

To list all enabled repositories:

```
# dnf repolist
```

4. Configure the repositories:

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-8-for-x86_64-baseos-eus-rpms \
    --enable=rhel-8-for-x86_64-appstream-eus-rpms \
    --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
    --enable=fast-datapath-for-rhel-8-x86_64-rpms \
    --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
    --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
    --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
    --enable=rhel-8-for-x86_64-appstream-tus-rpms \
    --enable=rhel-8-for-x86_64-baseos-tus-rpms
```

5. Set the RHEL version to 8.6:

```
# subscription-manager release --set=8.6
```

6. Enable version 12 of the **postgresql** module.

```
# dnf module -y enable postgresql:12
```

7. Enable version 14 of the **nodejs** module:

```
# dnf module -y enable nodejs:14
```

8. Synchronize installed packages to update them to the latest available versions.

```
# dnf distro-sync --nobest
```

Additional resources

For information on modules and module streams, see the following sections in *Installing, managing, and removing user-space components*

- Module streams
- Selecting a stream before installation of packages
- Resetting module streams
- Switching to a later stream

Initializing the PostgreSQL Database

1. Install the PostgreSQL server package:

   ```
   # dnf install postgresql-server postgresql-contrib
   ```

2. Initialize the PostgreSQL database instance:

   ```
   # postgresql-setup --initdb
   ```

3. Enable the **postgresql** service and configure it to start when the machine boots:

   ```
   # systemctl enable postgresql
   # systemctl start postgresql
   ```

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

   ```
   # su - postgres -c psql
   ```

5. Create a default user. The Manager’s default user is **engine**:

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

6. Create a database. The Manager’s default database name 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';
   ```

7. Connect to the new database:

   ```
   postgres=# \c database_name
   ```

8. Add the **uuid-ossp** extension:

   ```
   database_name=# CREATE EXTENSION "uuid-ossp";
   ```

9. Add the **plpgsql** language if it does not exist:

   ```
   database_name=# CREATE LANGUAGE plpgsql;
   ```

10. Quit the **psql** interface:

    ```
    database_name=# \q
    ```

11. Edit the **/var/lib/pgsql/data/pg_hba.conf** file to enable md5 client authentication, so that the engine can access the database remotely. Add the following line immediately below the line that starts with **local** at the bottom of the file. Replace **X.X.X.X** with the IP address of the Manager or Data Warehouse machine, and replace **0-32** or **0-128** with the CIDR mask length:

    ```
    host    database_name    user_name    X.X.X.X/0-32    md5
    host    database_name    user_name    X.X.X.X::/0-128   md5
    ```

For example:

```
# IPv4, 32-bit address:
host    engine    engine    192.168.12.10/32    md5

# IPv6, 128-bit address:
host    engine    engine    fe80::7a31:c1ff:0000:0000/96   md5
```

12. 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.

13. Update the PostgreSQL server's configuration. In the **/var/lib/pgsql/data/postgresql.conf** file, add the following lines to the bottom of the file:

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

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

    ```
    # firewall-cmd --zone=public --add-service=postgresql
    # firewall-cmd --permanent --zone=public --add-service=postgresql
    ```

15. Restart the **postgresql** service:

    ```
    # systemctl restart postgresql
    ```

16. Optionally, set up SSL to secure database connections.

3.4. INSTALLING AND CONFIGURING THE RED HAT VIRTUALIZATION MANAGER

Install the package and dependencies for the Red Hat Virtualization Manager, and configure it using the **engine-setup** command. The script 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.

IMPORTANT

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.

You can run **engine-setup --accept-defaults** to automatically accept all questions that have default answers. This option should be used with caution and only if you are familiar with **engine-setup**.

Procedure

1. Ensure all packages are up to date:

   ```
   # dnf upgrade --nobest
   ```

   NOTE

   Reboot the machine if any kernel-related packages were updated.

2. Install the **rhvm** package and dependencies.

   ```
   # dnf install rhvm
   ```

3. Run the **engine-setup** command to begin configuring the Red Hat Virtualization Manager:

   ```
   # engine-setup
   ```

4. Optional: Type **Yes** and press **Enter** to set up Cinderlib integration on this machine:

   ```
   Set up Cinderlib integration
   (Currently in tech preview)
   (Yes, No) [No]:
   ```

   IMPORTANT

   Cinderlib is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs), might not be functionally complete, and Red Hat does not recommend to use them for production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process. For more information on Red Hat Technology Preview features support scope, see Red Hat Technology Preview Features Support Scope.

5. Press **Enter** to configure the Manager on this machine:

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

6. Optional: Install Open Virtual Network (OVN). Selecting **Yes** installs an OVN server on the Manager machine and adds it to Red Hat Virtualization as an external network provider. This action also configures the Default cluster to use OVN as its default network provider.

   IMPORTANT

   Also see the "Next steps" in Adding Open Virtual Network (OVN) as an External Network Provider in the *Administration Guide*.

   ```
   Configuring ovirt-provider-ovn also sets the Default cluster's default network provider to ovirt-provider-ovn.
   Non-Default clusters may be configured with an OVN after installation.
   Configure ovirt-provider-ovn (Yes, No) [Yes]:
   ```

   For more information on using OVN networks in Red Hat Virtualization, see Adding Open Virtual Network (OVN) as an External Network Provider in the *Administration Guide*.

7. Optional: Allow **engine-setup** to configure a WebSocket Proxy server for allowing users to connect to virtual machines through the **noVNC** console:

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

   IMPORTANT

   The WebSocket Proxy and noVNC are Technology Preview features only. Technology Preview features are not supported with Red Hat production service-level agreements (SLAs) and might not be functionally complete, and Red Hat does not recommend using them for production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process. For more information see Red Hat Technology Preview Features Support Scope .

8. To configure Data Warehouse on a remote server, answer **No** and see Installing and Configuring Data Warehouse on a Separate Machine after completing the Manager configuration.

   ```
   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]:
   ```

   IMPORTANT

   Red Hat only supports installing the Data Warehouse database, the Data Warehouse service, and Grafana all on the same machine as each other.

9. To configure Grafana on the same machine as the Data Warehouse service, enter **No**:

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

10. Optional: Allow access to a virtual machine'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*.

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

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

12. The **engine-setup** command checks your firewall configuration and offers to open the ports used by the Manager for external communication, such as ports 80 and 443. If you do not allow **engine-setup** to modify your firewall configuration, you must manually open the ports used by the Manager. **firewalld** is configured as the firewall 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.

13. Specify whether to configure the Manager database on this machine, or on another machine:

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

    NOTE

    Deployment with a remote engine database is now deprecated. This functionality will be removed in a future release.

    If you select **Remote**, input the following values for the preconfigured remote database server. Replace **localhost** with the ip address or FQDN of the remote database server:

    ```
    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:
    ```

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

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

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

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

    - **Both** - offers the greatest flexibility. In most cases, select **Both**.

- **Virt** - allows you to run virtual machines in the environment.
- **Gluster** - only allows you to manage GlusterFS from the Administration Portal.

> NOTE
>
> GlusterFS Storage is deprecated, and will no longer be supported in future releases.

16. If you installed the OVN provider, you can choose to use the default credentials, or specify an alternative.

```
Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No) [Yes]:
oVirt OVN provider user[admin@internal]:
oVirt OVN provider password:
```

17. 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]:
```

18. 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]:
```

19. 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]:
```

20. 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]:
```

21. You can specify a unique password for the Grafana admin user, or use same one as the Manager admin password:

```
Use Engine admin password as initial Grafana admin password (Yes, No) [Yes]:
```

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

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

When your environment has been configured, **engine-setup** displays details about how to access your environment.

Next steps

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. **engine-setup** 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.

- 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.

- Install the certificate authority according to the instructions provided by your browser. You can get the certificate authority's certificate by navigating to **http://<manager-fqdn>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA**, replacing <manager-fqdn> with the FQDN that you provided during the installation.

Install the Data Warehouse service and database on the remote server:

3.5. INSTALLING AND CONFIGURING DATA WAREHOUSE ON A SEPARATE MACHINE

This section describes installing and configuring the Data Warehouse service on a separate machine from the Red Hat Virtualization Manager. Installing Data Warehouse on a separate machine helps to reduce the load on the Manager machine.

> **NOTE**
>
> Red Hat only supports installing the Data Warehouse database, the Data Warehouse service and Grafana all on the same machine as each other, even though you can install each of these components on separate machines from each other.

Prerequisites

- The Red Hat Virtualization Manager is installed on a separate machine.

- A physical server or virtual machine running Red Hat Enterprise Linux 8.

- The Manager database password.

Enabling the Red Hat Virtualization Manager Repositories

You need to log in and register the Data Warehouse machine with Red Hat Subscription Manager, attach the **Red Hat Virtualization Manager** subscription, 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
```

NOTE

If you are using an IPv6 network, use an IPv6 transition mechanism to access the Content Delivery Network and subscription manager.

2. Find the **Red Hat Virtualization Manager** subscription pool and record the pool ID:

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

3. Use the pool ID to attach the subscription to the system:

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

NOTE

To view currently attached subscriptions:

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

To list all enabled repositories:

```
# dnf repolist
```

4. Configure the repositories:

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-8-for-x86_64-baseos-eus-rpms \
    --enable=rhel-8-for-x86_64-appstream-eus-rpms \
    --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
    --enable=fast-datapath-for-rhel-8-x86_64-rpms \
    --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
    --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
    --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
    --enable=rhel-8-for-x86_64-appstream-tus-rpms \
    --enable=rhel-8-for-x86_64-baseos-tus-rpms
```

5. Set the RHEL version to 8.6:

```
# subscription-manager release --set=8.6
```

6. Enable the **pki-deps** module.

```
# dnf module -y enable pki-deps
```

7. Enable version 12 of the **postgresql** module.

```
# dnf module -y enable postgresql:12
```

8. Enable version 14 of the **nodejs** module:

```
# dnf module -y enable nodejs:14
```

9. Synchronize installed packages to update them to the latest available versions.

```
# dnf distro-sync --nobest
```

Additional resources

For information on modules and module streams, see the following sections in *Installing, managing, and removing user-space components*

- Module streams
- Selecting a stream before installation of packages
- Resetting module streams
- Switching to a later stream

Installing Data Warehouse on a Separate Machine

Procedure

1. Log in to the machine where you want to install the database.
2. Ensure that all packages are up to date:

```
# dnf upgrade --nobest
```

3. Install the **ovirt-engine-dwh-setup** package:

```
# dnf install ovirt-engine-dwh-setup
```

4. Run the **engine-setup** command to begin the installation:

```
# engine-setup
```

5. Answer **Yes** to install Data Warehouse on this machine:

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

6. Answer **Yes** to install Grafana on this machine:

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

7. Press **Enter** to accept the automatically-detected host name, or enter an alternative host name and press **Enter**:

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

8. Press **Enter** to automatically configure the firewall, or type **No** and press **Enter** to maintain existing settings:

```
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. Enter the fully qualified domain name of the Manager machine, and then press **Enter**:

   ```
   Host fully qualified DNS name of the engine server []:
   ```

10. Press **Enter** to allow setup to sign the certificate on the Manager via SSH:

    ```
    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]:
    ```

11. Press **Enter** to accept the default SSH port, or enter an alternative port number and then press **Enter**:

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

12. Enter the root password for the Manager machine:

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

13. Specify whether to host the Data Warehouse database on this machine (Local), or on another machine (Remote).:

    NOTE

    Red Hat only supports installing the Data Warehouse database, the Data Warehouse service and Grafana all on the same machine as each other, even though you can install each of these components on separate machines from each other.

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

    - If you select **Local**, the **engine-setup** script 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]:
      ```

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

- If you select **Remote**, you are prompted to provide details about the remote database host. Input the following values for the preconfigured remote database host:

  ```
  DWH database host []: dwh-db-fqdn
  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: password
  ```

- If you select **Remote**, you are prompted to enter the username and password for the Grafana database user:

  ```
  Grafana database user [ovirt_engine_history_grafana]:
  Grafana database password:
  ```

14. Enter the fully qualified domain name and password for the Manager database machine. If you are installing the Data Warehouse database on the same machine where the Manager database is installed, use the same FQDN. Press **Enter** to accept the default values in each other field:

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

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

    ```
    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 Application Settings for the Data Warehouse service in ovirt-engine-dwhd.conf (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. Use **Basic** when the Manager and Data Warehouse are installed on the same machine.

16. Confirm your installation settings:

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

17. After the Data Warehouse configuration is complete, on the Red Hat Virtualization Manager, restart the **ovirt-engine** service:

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

18. Optionally, set up SSL to secure database connections.

Log in to the Administration Portal, where you can add hosts and storage to the environment:

3.6. CONNECTING TO THE ADMINISTRATION PORTAL

Access the Administration Portal using a web browser.

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

    > **NOTE**
    >
    > You can access the Administration Portal using alternate host names or IP addresses. To do so, you need to add a configuration file under **/etc/ovirt-engine/engine.conf.d/**. For example:
    >
    > ```
    > # vi /etc/ovirt-engine/engine.conf.d/99-custom-sso-setup.conf
    > SSO_ALTERNATE_ENGINE_FQDNS="alias1.example.com
    > alias2.example.com"
    > ```
    >
    > The list of alternate host names needs to be separated by spaces. You can also add the IP address of the Manager to the list, but using IP addresses instead of DNS-resolvable host names is not recommended.

2. Click **Administration Portal**. An SSO login page displays. SSO login enables you to log in to the Administration and VM Portal 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** along with the password that you specified during installation.

4. Select the **Domain** to authenticate against. 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 is chosen based on the locale settings of your web browser. If you want 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.

CHAPTER 4. INSTALLING HOSTS FOR RED HAT VIRTUALIZATION

Red Hat Virtualization supports two types of hosts: Red Hat Virtualization Hosts (RHVH) and Red Hat Enterprise Linux hosts. Depending on your environment, you may want to use one type only, or both. At least two hosts are required for features such as migration and high availability.

See Recommended practices for configuring host networks for networking information.

IMPORTANT

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

Table 4.1. Host Types

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 host, thick host	Red Hat Enterprise Linux systems with the appropriate subscriptions attached can be used as hosts.

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 earlier compatibility version, you must create additional data centers and clusters. For more information about compatibility versions see *Red Hat Virtualization Manager Compatibility* in Red Hat Virtualization Life Cycle .

4.1. RED HAT VIRTUALIZATION HOSTS

4.1.1. Installing Red Hat Virtualization Hosts

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 web interface for monitoring the host and performing administrative tasks. See Running Cockpit 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.

The host must meet the minimum host requirements.

WARNING

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

Procedure

1. Go to the Get Started with Red Hat Virtualization on the Red Hat Customer Portal and log in.
2. Click **Download Latest** to access the product download page.
3. Choose the appropriate **Hypervisor Image for RHV** from the list and click **Download Now**.
4. Start the machine on which you are installing RHVH, booting from the prepared installation media.
5. From the boot menu, select **Install RHVH 4.4** 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.

6. Select a language, and click **Continue**.
7. Select a keyboard layout from the **Keyboard Layout** screen and click **Done**.
8. Select the device on which to install RHVH from the **Installation Destination** screen. Optionally, enable encryption. Click **Done**.

   IMPORTANT

   Use the **Automatically configure partitioning** option.

9. Select a time zone from the **Time & Date** screen and click **Done**.
10. Select a network from the **Network & Host Name** screen and click **Configure...** to configure the connection details.

NOTE

To use the connection every time the system boots, select the **Connect automatically with priority** check box. For more information, see Configuring network and host name options in the *Red Hat Enterprise Linux 8 Installation Guide*.

Enter a host name in the **Host Name** field, and click **Done**.

11. Optional: Configure **Security Policy** and **Kdump**. See Customizing your RHEL installation using the GUI in *Performing a standard RHEL installation* for Red Hat Enterprise Linux 8 for more information on each of the sections in the **Installation Summary** screen.

12. Click **Begin Installation**.

13. Set a root password and, optionally, create an additional user while RHVH installs.

WARNING

Do not create untrusted users on RHVH, as this can lead to exploitation of local security vulnerabilities.

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

NOTE

When RHVH restarts, **nodectl check** performs a health check on the host and displays the result when you log in on the command line. The message **node status: OK** or **node status: DEGRADED** indicates the health status. Run **nodectl check** to get more information.

NOTE

If necessary, you can prevent kernel modules from loading automatically.

4.1.2. Enabling the Red Hat Virtualization Host Repository

Register the system to receive updates. Red Hat Virtualization Host only requires one repository. This section provides instructions for registering RHVH with the Content Delivery Network, or with Red Hat Satellite 6.

Registering RHVH with the Content Delivery Network

1. Enable the **Red Hat Virtualization Host 8** repository to allow later updates to the Red Hat Virtualization Host:

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

Registering RHVH with Red Hat Satellite 6

1. Log in to the Cockpit web interface at **https://*HostFQDNorIP*:9090**.
2. Click **Terminal**.
3. Register RHVH with Red Hat Satellite 6:

```
# rpm -Uvh http://satellite.example.com/pub/katello-ca-consumer-latest.noarch.rpm
# subscription-manager register --org="org_id"
# subscription-manager list --available
# subscription-manager attach --pool=pool_id
# subscription-manager repos \
  --disable='*' \
  --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

> NOTE
>
> You can also configure virtual machine subscriptions in Red Hat Satellite using virt-who. See Using virt-who to manage host-based subscriptions .

4.1.3. Advanced Installation

4.1.3.1. Custom Partitioning

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

If your installation requires custom partitioning, select the **I will configure partitioning** option during the installation, and note that the following restrictions apply:

- Ensure the default **LVM Thin Provisioning** option is selected in the **Manual Partitioning** window.
- The following directories are required and must be on thin provisioned logical volumes:
    - root (/)
    - **/home**
    - **/tmp**
    - **/var**
    - **/var/crash**
    - **/var/log**
    - **/var/log/audit**

> IMPORTANT
>
> Do not create a separate partition for **/usr**. Doing so will cause the installation to fail.
>
> **/usr** must be on a logical volume that is able to change versions along with RHVH, and therefore should be left on root (/).

For information about the required storage sizes for each partition, see Storage Requirements.

- The /**boot** directory should be defined as a standard partition.
- The /**var** directory must be on a separate volume or disk.
- Only XFS or Ext4 file systems are supported.

Configuring Manual Partitioning in a Kickstart File

The following example demonstrates how to configure manual partitioning in a Kickstart file.

```
clearpart --all
part /boot --fstype xfs --size=1000 --ondisk=sda
part pv.01 --size=42000 --grow
volgroup HostVG pv.01 --reserved-percent=20
logvol swap --vgname=HostVG --name=swap --fstype=swap --recommended
logvol none --vgname=HostVG --name=HostPool --thinpool --size=40000 --grow
logvol / --vgname=HostVG --name=root --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=6000 --grow
logvol /var --vgname=HostVG --name=var --thin --fstype=ext4 --poolname=HostPool
--fsoptions="defaults,discard" --size=15000
logvol /var/crash --vgname=HostVG --name=var_crash --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=10000
logvol /var/log --vgname=HostVG --name=var_log --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=8000
logvol /var/log/audit --vgname=HostVG --name=var_audit --thin --fstype=ext4 --poolname=HostPool -
-fsoptions="defaults,discard" --size=2000
logvol /home --vgname=HostVG --name=home --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=1000
logvol /tmp --vgname=HostVG --name=tmp --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=1000
```

NOTE

If you use **logvol --thinpool --grow**, you must also include **volgroup --reserved-space** or **volgroup --reserved-percent** to reserve space in the volume group for the thin pool to grow.

4.1.3.2. Installing a DUD driver on a host without installer support

There are times when installing Red Hat Virtualization Host (RHVH) requires a Driver Update Disk (DUD), such as when using a hardware RAID device that is not supported by the default configuration of RHVH. In contrast with Red Hat Enterprise Linux hosts, RHVH does not fully support using a DUD. Subsequently the host fails to boot normally after installation because it does not see RAID. Instead it boots into emergency mode.

Example output:

```
Warning: /dev/test/rhvh-4.4-20210202.0+1 does not exist
Warning: /dev/test/swap does not exist
Entering emergency mode. Exit the shell to continue.
```

In such a case you can manually add the drivers before finishing the installation.

Prerequisites

- A machine onto which you are installing RHVH.
- A DUD.
- If you are using a USB drive for the DUD and RHVH, you must have at least two available USB ports.

Procedure

1. Load the DUD on the host machine.
2. Install RHVH. See Installing Red Hat Virtualization Hosts in *Installing Red Hat Virtualization as a self-hosted engine using the command line*.

   IMPORTANT

   When installation completes, do not reboot the system.

   TIP

   If you want to access the DUD using SSH, do the following:

   - Add the string **inst.sshd** to the kernel command line:

     ```
     <kernel_command_line> inst.sshd
     ```

   - Enable networking during the installation.

3. Enter the console mode, by pressing **Ctrl** + **Alt** + **F3**. Alternatively you can connect to it using SSH.
4. Mount the DUD:

   ```
   # mkdir /mnt/dud
   # mount -r /dev/<dud_device> /mnt/dud
   ```

5. Copy the RPM file inside the DUD to the target machine's disk:

   ```
   # cp /mnt/dud/rpms/<path>/<rpm_file>.rpm /mnt/sysroot/root/
   ```

   For example:

   ```
   # cp /mnt/dud/rpms/x86_64/kmod-3w-9xxx-2.26.02.014-5.el8_3.elrepo.x86_64.rpm
   /mnt/sysroot/root/
   ```

6. Change the root directory to **/mnt/sysroot**:

   ```
   # chroot /mnt/sysroot
   ```

7. Back up the current initrd images. For example:

```
# cp -p /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img /boot/initramfs-4.18.0-
240.15.1.el8_3.x86_64.img.bck1
# cp -p /boot/rhvh-4.4.5.1-0.20210323.0+1/initramfs-4.18.0-240.15.1.el8_3.x86_64.img
/boot/rhvh-4.4.5.1-0.20210323.0+1/initramfs-4.18.0-240.15.1.el8_3.x86_64.img.bck1
```

8. Install the RPM file for the driver from the copy you made earlier.
   For example:

```
# dnf install /root/kmod-3w-9xxx-2.26.02.014-5.el8_3.elrepo.x86_64.rpm
```

NOTE

This package is not visible on the system after you reboot into the installed environment, so if you need it, for example, to rebuild the **initramfs**, you need to install that package once again, after which the package remains.

If you update the host using **dnf**, the driver update persists, so you do not need to repeat this process.

TIP

If you do not have an internet connection, use the **rpm** command instead of **dnf**:

```
# rpm -ivh /root/kmod-3w-9xxx-2.26.02.014-5.el8_3.elrepo.x86_64.rpm
```

9. Create a new image, forcefully adding the driver:

```
# dracut --force --add-drivers <module_name> --kver <kernel_version>
```

For example:

```
# dracut --force --add-drivers 3w-9xxx --kver 4.18.0-240.15.1.el8_3.x86_64
```

10. Check the results. The new image should be larger, and include the driver. For example, compare the sizes of the original, backed-up image file and the new image file.
    In this example, the new image file is 88739013 bytes, larger than the original 88717417 bytes:

```
# ls -ltr /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img*
-rw-------. 1 root root 88717417 Jun  2 14:29 /boot/initramfs-4.18.0-
240.15.1.el8_3.x86_64.img.bck1
-rw-------. 1 root root 88739013 Jun  2 17:47 /boot/initramfs-4.18.0-
240.15.1.el8_3.x86_64.img
```

The new drivers should be part of the image file. For example, the 3w-9xxx module should be included:

```
# lsinitrd /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img | grep 3w-9xxx
drwxr-xr-x   2 root     root            0 Feb 22 15:57 usr/lib/modules/4.18.0-
240.15.1.el8_3.x86_64/weak-updates/3w-9xxx
lrwxrwxrwx   1 root     root           55 Feb 22 15:57 usr/lib/modules/4.18.0-
240.15.1.el8_3.x86_64/weak-updates/3w-9xxx/3w-9xxx.ko-../../../4.18.0-
```

```
240.el8.x86_64/extra/3w-9xxx/3w-9xxx.ko
drwxr-xr-x   2 root     root           0 Feb 22 15:57 usr/lib/modules/4.18.0-
240.el8.x86_64/extra/3w-9xxx
-rw-r--r--   1 root     root       80121 Nov 10  2020 usr/lib/modules/4.18.0-
240.el8.x86_64/extra/3w-9xxx/3w-9xxx.ko
```

11. Copy the image to the the directory under **/boot** that contains the kernel to be used in the layer being installed, for example:

    ```
    # cp -p /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img /boot/rhvh-4.4.5.1-
    0.20210323.0+1/initramfs-4.18.0-240.15.1.el8_3.x86_64.img
    ```

12. Exit chroot.

13. Exit the shell.

14. If you used **Ctrl** + **Alt** + **F3** to access a virtual terminal, then move back to the installer by pressing **Ctrl** + **Alt** + **F_<n>_**, usually **F1** or **F5**

15. At the installer screen, reboot.

Verification

The machine should reboot successfully.

4.1.3.3. Automating Red Hat Virtualization Host deployment

You can install Red Hat Virtualization Host (RHVH) without a physical media device by booting from a PXE server over the network with a Kickstart file that contains the answers to the installation questions.

> **WARNING**
>
> When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

General instructions for installing from a PXE server with a Kickstart file are available in the *Red Hat Enterprise Linux Installation Guide*, as RHVH is installed in much the same way as Red Hat Enterprise Linux. RHVH-specific instructions, with examples for deploying RHVH with Red Hat Satellite, are described below.

The automated RHVH deployment has 3 stages:

- Preparing the Installation Environment
- Configuring the PXE Server and the Boot Loader
- Creating and Running a Kickstart File

4.1.3.3.1. Preparing the installation environment

1. Go to the Get Started with Red Hat Virtualization on the Red Hat Customer Portal and log in.

2. Click **Download Latest** to access the product download page.

3. Choose the appropriate **Hypervisor Image for RHV** from the list and click **Download Now**.

4. Make the RHVH ISO image available over the network. See Installation Source on a Network in the *Red Hat Enterprise Linux Installation Guide* .

5. Extract the **squashfs.img** hypervisor image file from the RHVH ISO:

```
# mount -o loop /path/to/RHVH-ISO /mnt/rhvh
# cp /mnt/rhvh/Packages/redhat-virtualization-host-image-update* /tmp
# cd /tmp
# rpm2cpio redhat-virtualization-host-image-update* | cpio -idmv
```

NOTE

This **squashfs.img** file, located in the **/tmp/usr/share/redhat-virtualization-host/image/** directory, is called **redhat-virtualization-host-*version_number*_version.squashfs.img**. It contains the hypervisor image for installation on the physical machine. It should not be confused with the **/LiveOS/squashfs.img** file, which is used by the Anaconda **inst.stage2** option.

4.1.3.3.2. Configuring the PXE server and the boot loader

1. Configure the PXE server. See Preparing for a Network Installation in the *Red Hat Enterprise Linux Installation Guide*.

2. Copy the RHVH boot images to the **/tftpboot** directory:

```
# cp mnt/rhvh/images/pxeboot/{vmlinuz,initrd.img} /var/lib/tftpboot/pxelinux/
```

3. Create a **rhvh** label specifying the RHVH boot images in the boot loader configuration:

```
LABEL rhvh
MENU LABEL Install Red Hat Virtualization Host
KERNEL /var/lib/tftpboot/pxelinux/vmlinuz
APPEND initrd=/var/lib/tftpboot/pxelinux/initrd.img inst.stage2=URL/to/RHVH-ISO
```

RHVH Boot loader configuration example for Red Hat Satellite

If you are using information from Red Hat Satellite to provision the host, you must create a global or host group level parameter called **rhvh_image** and populate it with the directory URL where the ISO is mounted or extracted:

```
<%#
kind: PXELinux
name: RHVH PXELinux
%>
# Created for booting new hosts
#
```

```
DEFAULT rhvh

LABEL rhvh
KERNEL <%= @kernel %>
APPEND initrd=<%= @initrd %> inst.ks=<%= foreman_url("provision") %> inst.stage2=<%=
@host.params["rhvh_image"] %> intel_iommu=on console=tty0 console=ttyS1,115200n8
ssh_pwauth=1 local_boot_trigger=<%= foreman_url("built") %>
IPAPPEND 2
```

4. Make the content of the RHVH ISO locally available and export it to the network, for example, using an HTTPD server:

```
# cp -a /mnt/rhvh/ /var/www/html/rhvh-install
# curl URL/to/RHVH-ISO/rhvh-install
```

4.1.3.3.3. Creating and running a Kickstart file

1. Create a Kickstart file and make it available over the network. See Kickstart Installations in the *Red Hat Enterprise Linux Installation Guide* .

2. Ensure that the Kickstart file meets the following RHV-specific requirements:

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

     ```
     liveimg --url=example.com/tmp/usr/share/redhat-virtualization-host/image/redhat-
     virtualization-host-version_number_version.squashfs.img
     ```

   - Autopartitioning is highly recommended, but use caution: ensure that the local disk is detected first, include the **ignoredisk** command, and specify the local disk to ignore, such as **sda**. To ensure that a particular drive is used, Red Hat recommends using **ignoredisk --only-use=/dev/disk/<*path*>** or **ignoredisk --only-use=/dev/disk/<*ID*>**:

     ```
     autopart --type=thinp
     ignoredisk --only-use=sda
     ignoredisk --only-use=/dev/disk/<path>
     ignoredisk --only-use=/dev/disk/<ID>
     ```

     NOTE

     Autopartitioning requires thin provisioning.

     The **--no-home** option does not work in RHVH because **/home** is a required directory.

     If your installation requires manual partitioning, see Custom Partitioning for a list of limitations that apply to partitions and an example of manual partitioning in a Kickstart file.

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

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

–

NOTE

Ensure that the **nodectl init** command is at the very end of the **%post** section but before the reboot code, if any.

Kickstart example for deploying RHVH on its own

This Kickstart example shows you how to deploy RHVH. You can include additional commands and options as required.

WARNING

This example assumes that all disks are empty and can be initialized. If you have attached disks with data, either remove them or add them to the **ignoredisks** property.

```
liveimg --url=http://FQDN/tmp/usr/share/redhat-virtualization-host/image/redhat-virtualization-host-version_number_version.squashfs.img
clearpart --all
autopart --type=thinp
rootpw --plaintext ovirt
timezone --utc America/Phoenix
zerombr
text

reboot

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

Kickstart example for deploying RHVH with registration and network configuration from Satellite

This Kickstart example uses information from Red Hat Satellite to configure the host network and register the host to the Satellite server. You must create a global or host group level parameter called **rhvh_image** and populate it with the directory URL to the **squashfs.img** file. **ntp_server1** is also a global or host group level variable.

WARNING

This example assumes that all disks are empty and can be initialized. If you have attached disks with data, either remove them or add them to the **ignoredisks** property.

```
<%#
kind: provision
name: RHVH Kickstart default
oses:
- RHVH
%>
install
liveimg --url=<%= @host.params['rhvh_image'] %>squashfs.img

network --bootproto static --ip=<%= @host.ip %> --netmask=<%= @host.subnet.mask
%> --gateway=<%= @host.subnet.gateway %> --nameserver=<%=
@host.subnet.dns_primary %> --hostname <%= @host.name %>

zerombr
clearpart --all
autopart --type=thinp

rootpw --iscrypted <%= root_pass %>

# installation answers
lang en_US.UTF-8
timezone <%= @host.params['time-zone'] || 'UTC' %>
keyboard us
firewall --service=ssh
services --enabled=sshd

text
reboot

%post --log=/root/ks.post.log --erroronfail
nodectl init
<%= snippet 'subscription_manager_registration' %>
<%= snippet 'kickstart_networking_setup' %>
/usr/sbin/ntpdate -sub <%= @host.params['ntp_server1'] || '0.fedora.pool.ntp.org' %>
/usr/sbin/hwclock --systohc

/usr/bin/curl <%= foreman_url('built') %>

sync
systemctl reboot
%end
```

3. Add the Kickstart file location to the boot loader configuration file on the PXE server:

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

4. Install RHVH following the instructions in Booting from the Network Using PXE in the *Red Hat Enterprise Linux Installation Guide*.

4.2. RED HAT ENTERPRISE LINUX HOSTS

4.2.1. Installing Red Hat Enterprise Linux hosts

A Red Hat Enterprise Linux host is based on a standard basic installation of Red Hat Enterprise Linux 8 on a physical server, with the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscriptions attached.

For detailed installation instructions, see the *Performing a standard RHEL installation* .

The host must meet the minimum host requirements.

WARNING

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

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

Do not install third-party watchdogs on Red Hat Enterprise Linux hosts. They can interfere with the watchdog daemon provided by VDSM.

4.2.2. Enabling the Red Hat Enterprise Linux host Repositories

To use a Red Hat Enterprise Linux machine as a host, you must register the system with the Content Delivery Network, attach the **Red Hat Enterprise Linux Server** and **Red Hat Virtualization** subscriptions, and enable the host 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=poolid
```

NOTE

To view currently attached subscriptions:

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

To list all enabled repositories:

```
# dnf repolist
```

4. Configure the repositories:

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-8-for-x86_64-baseos-eus-rpms \
    --enable=rhel-8-for-x86_64-appstream-eus-rpms \
    --enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
    --enable=fast-datapath-for-rhel-8-x86_64-rpms \
    --enable=advanced-virt-for-rhel-8-x86_64-rpms \
    --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
    --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
    --enable=rhel-8-for-x86_64-appstream-tus-rpms \
    --enable=rhel-8-for-x86_64-baseos-tus-rpms
```

For Red Hat Enterprise Linux 8 hosts, little endian, on IBM POWER8 or IBM POWER9 hardware:

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhv-4-mgmt-agent-for-rhel-8-ppc64le-rpms \
    --enable=rhv-4-tools-for-rhel-8-ppc64le-rpms \
    --enable=advanced-virt-for-rhel-8-ppc64le-rpms \
    --enable=rhel-8-for-ppc64le-appstream-rpms \
    --enable=rhel-8-for-ppc64le-baseos-rpms \
    --enable=fast-datapath-for-rhel-8-ppc64le-rpms \
```

5. Set the RHEL version to 8.6:

```
# subscription-manager release --set=8.6
```

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

```
# dnf upgrade --nobest
```

7. Reboot the machine.

NOTE

If necessary, you can prevent kernel modules from loading automatically.

4.2.3. Installing Cockpit on Red Hat Enterprise Linux hosts

You can install Cockpit for monitoring the host’s resources and performing administrative tasks.

Procedure

1. Install the dashboard packages:

   ```
   # dnf install cockpit-ovirt-dashboard
   ```

2. Enable and start the **cockpit.socket** service:

   ```
   # systemctl enable cockpit.socket
   # systemctl start cockpit.socket
   ```

3. Check if Cockpit is an active service in the firewall:

   ```
   # firewall-cmd --list-services
   ```

   You should see **cockpit** listed. If it is not, enter the following with root permissions to add **cockpit** as a service to your firewall:

   ```
   # firewall-cmd --permanent --add-service=cockpit
   ```

   The **--permanent** option keeps the **cockpit** service active after rebooting.

You can log in to the Cockpit web interface at **https://*HostFQDNorIP*:9090**.

4.3. RECOMMENDED PRACTICES FOR CONFIGURING HOST NETWORKS

> **IMPORTANT**
>
> Always use the RHV Manager to modify the network configuration of hosts in your clusters. Otherwise, you might create an unsupported configuration. For details, see Network Manager Stateful Configuration (nmstate) .

If your network environment is complex, you may need to configure a host network manually before adding the host to the Red Hat Virtualization Manager.

Consider the following practices for configuring a host network:

- Configure the network with Cockpit. Alternatively, you can use **nmtui** or **nmcli**.
- If a network is not required for a self-hosted engine deployment or for adding a host to the Manager, configure the network in the Administration Portal after adding the host to the Manager. See Creating a New Logical Network in a Data Center or Cluster .
- Use the following naming conventions:
  - VLAN devices: ***VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD***
  - VLAN interfaces: ***physical_device*.*VLAN_ID*** (for example, **eth0.23**, **eth1.128**, **enp3s0.50**)
  - Bond interfaces: **bond*number*** (for example, **bond0**, **bond1**)
  - VLANs on bond interfaces: **bond*number*.*VLAN_ID*** (for example, **bond0.50**, **bond1.128**)

- Use network bonding. Network teaming is not supported in Red Hat Virtualization and will cause errors if the host is used to deploy a self-hosted engine or added to the Manager.
- Use recommended bonding modes:
  - If the **ovirtmgmt** network is not used by virtual machines, the network may use any supported bonding mode.
  - If the **ovirtmgmt** network is used by virtual machines, see *Which bonding modes work when used with a bridge that virtual machine guests or containers connect to?*.
  - Red Hat Virtualization's default bonding mode is **(Mode 4) Dynamic Link Aggregation**. If your switch does not support Link Aggregation Control Protocol (LACP), use **(Mode 1) Active-Backup**. See Bonding Modes for details.
- Configure a VLAN on a physical NIC as in the following example (although **nmcli** is used, you can use any tool):

```
# nmcli connection add type vlan con-name vlan50 ifname eth0.50 dev eth0 id 50
# nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24 +ipv4.gateway 123.123.0.254
```

- Configure a VLAN on a bond as in the following example (although **nmcli** is used, you can use any tool):

```
# nmcli connection add type bond con-name bond0 ifname bond0 bond.options "mode=active-backup,miimon=100" ipv4.method disabled ipv6.method ignore
# nmcli connection add type ethernet con-name eth0 ifname eth0 master bond0 slave-type bond
# nmcli connection add type ethernet con-name eth1 ifname eth1 master bond0 slave-type bond
# nmcli connection add type vlan con-name vlan50 ifname bond0.50 dev bond0 id 50
# nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24 +ipv4.gateway 123.123.0.254
```

- Do not disable **firewalld**.
- Customize the firewall rules in the Administration Portal after adding the host to the Manager. See Configuring Host Firewall Rules.

4.4. ADDING STANDARD HOSTS TO THE RED HAT VIRTUALIZATION MANAGER

> **IMPORTANT**
>
> Always use the RHV Manager to modify the network configuration of hosts in your clusters. Otherwise, you might create an unsupported configuration. For details, see Network Manager Stateful Configuration (nmstate).

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, and creation of a bridge.

Procedure

1. From the Administration Portal, click **Compute** → **Hosts**.
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. Optionally, click the **Advanced Parameters** button to change the following advanced host settings:
   - Disable automatic firewall configuration.
   - 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 **Events** section of the **Notification Drawer** (🔔). After a brief delay the host status changes to **Up**.

CHAPTER 5. PREPARING STORAGE FOR RED HAT VIRTUALIZATION

You need to prepare storage to be used for storage domains in the new environment. A Red Hat Virtualization environment must have at least one data storage domain, but adding more is recommended.

> **WARNING**
>
> When installing or reinstalling the host’s operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

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 while active (but can be migrated between data centers). Data domains of multiple storage types can be added to the same data center, provided they are all shared, rather than local, domains.

You can use one of the following storage types:

- NFS
- iSCSI
- Fibre Channel (FCP)
- POSIX-compliant file system
- Local storage
- Red Hat Gluster Storage

5.1. PREPARING NFS STORAGE

Set up NFS shares on your file storage or remote server to serve as storage domains on Red Hat Enterprise Virtualization Host systems. After exporting the shares on the remote storage and configuring them in the Red Hat Virtualization Manager, the shares will be automatically imported on the Red Hat Virtualization hosts.

For information on setting up, configuring, mounting and exporting NFS, see *Managing file systems* for Red Hat Enterprise Linux 8.

Specific system user accounts and system user groups are required by Red Hat Virtualization so the Manager can store data in the storage domains represented by the exported directories. The following procedure sets the permissions for one directory. You must repeat the **chown** and **chmod** steps for all of the directories you intend to use as storage domains in Red Hat Virtualization.

Prerequisites

1. Install the NFS **utils** package.

   ```
   # dnf install nfs-utils -y
   ```

2. To check the enabled versions:

   ```
   # cat /proc/fs/nfsd/versions
   ```

3. Enable the following services:

   ```
   # systemctl enable nfs-server
   # systemctl enable rpcbind
   ```

Procedure

1. Create the group **kvm**:

   ```
   # groupadd kvm -g 36
   ```

2. Create the user **vdsm** in the group **kvm**:

   ```
   # useradd vdsm -u 36 -g kvm
   ```

3. Create the **storage** directory and modify the access rights.

   ```
   # mkdir /storage
   # chmod 0755 /storage
   # chown 36:36 /storage/
   ```

4. Add the **storage** directory to **/etc/exports** with the relevant permissions.

   ```
   # vi /etc/exports
   # cat /etc/exports
    /storage *(rw)
   ```

5. Restart the following services:

   ```
   # systemctl restart rpcbind
   # systemctl restart nfs-server
   ```

6. To see which export are available for a specific IP address:

   ```
   # exportfs
    /nfs_server/srv
                   10.46.11.3/24
    /nfs_server       <world>
   ```

NOTE

If changes in **/etc/exports** have been made after starting the services, the **exportfs -ra** command can be used to reload the changes. After performing all the above stages, the exports directory should be ready and can be tested on a different host to check that it is usable.

5.2. PREPARING ISCSI STORAGE

Red Hat Virtualization supports iSCSI storage, which is a storage domain created from a volume group made up of LUNs. Volume groups and LUNs cannot be attached to more than one storage domain at a time.

For information on setting up and configuring iSCSI storage, see Configuring an iSCSI target in *Managing storage devices* for Red Hat Enterprise Linux 8.

IMPORTANT

If you are using block storage and intend to deploy virtual machines on raw devices or direct LUNs and manage them with the Logical Volume Manager (LVM), you must create a filter to hide guest logical volumes. This will prevent guest logical volumes from being activated when the host is booted, a situation that could lead to stale logical volumes and cause data corruption. Use the **vdsm-tool config-lvm-filter** command to create filters for the LVM. See Creating an LVM filter

IMPORTANT

Red Hat Virtualization currently does not support block storage with a block size of 4K. You must configure block storage in legacy (512b block) mode.

IMPORTANT

If your host is booting from SAN storage and loses connectivity to the storage, the storage file systems become read-only and remain in this state after connectivity is restored.

To prevent this situation, add a drop-in multipath configuration file on the root file system of the SAN for the boot LUN to ensure that it is queued when there is a connection:

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
    multipath {
        wwid boot_LUN_wwid
        no_path_retry queue
    }
```

5.3. PREPARING FCP STORAGE

Red Hat Virtualization 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 on setting up and configuring FCP or multipathing on Red Hat Enterprise Linux, see the *Storage Administration Guide* and *DM Multipath Guide*.

IMPORTANT

If you are using block storage and intend to deploy virtual machines on raw devices or direct LUNs and manage them with the Logical Volume Manager (LVM), you must create a filter to hide guest logical volumes. This will prevent guest logical volumes from being activated when the host is booted, a situation that could lead to stale logical volumes and cause data corruption. Use the **vdsm-tool config-lvm-filter** command to create filters for the LVM. See Creating an LVM filter

IMPORTANT

Red Hat Virtualization currently does not support block storage with a block size of 4K. You must configure block storage in legacy (512b block) mode.

IMPORTANT

If your host is booting from SAN storage and loses connectivity to the storage, the storage file systems become read-only and remain in this state after connectivity is restored.

To prevent this situation, add a drop-in multipath configuration file on the root file system of the SAN for the boot LUN to ensure that it is queued when there is a connection:

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
    multipath {
        wwid boot_LUN_wwid
        no_path_retry queue
    }
  }
```

5.4. PREPARING POSIX-COMPLIANT FILE SYSTEM STORAGE

POSIX file system support allows you to mount file systems using the same mount options that you would normally use when mounting them manually from the command line. This functionality is intended to allow access to storage not exposed using NFS, iSCSI, or FCP.

Any POSIX-compliant file system used as a storage domain in Red Hat Virtualization must be a clustered file system, such as Global File System 2 (GFS2), and must support sparse files and direct I/O. The Common Internet File System (CIFS), for example, does not support direct I/O, making it incompatible with Red Hat Virtualization.

For information on setting up and configuring POSIX-compliant file system storage, see *Red Hat Enterprise Linux Global File System 2*.

IMPORTANT

Do **not** mount NFS storage by creating a POSIX-compliant file system storage domain. Always create an NFS storage domain instead.

5.5. PREPARING LOCAL STORAGE

On Red Hat Virtualization Host (RHVH), local storage should always be defined on a file system that is separate from / (root). Use a separate logical volume or disk, to prevent possible loss of data during upgrades.

Procedure for Red Hat Enterprise Linux hosts

1. On the host, create the directory to be used for the local storage:

   ```
   # mkdir -p /data/images
   ```

2. Ensure that the directory has permissions allowing read/write access to the **vdsm** user (UID 36) and **kvm** group (GID 36):

   ```
   # chown 36:36 /data /data/images
   # chmod 0755 /data /data/images
   ```

Procedure for Red Hat Virtualization Hosts

Create the local storage on a logical volume:

1. Create a local storage directory:

   ```
   # mkdir /data
   # lvcreate -L $SIZE rhvh -n data
   # mkfs.ext4 /dev/mapper/rhvh-data
   # echo "/dev/mapper/rhvh-data /data ext4 defaults,discard 1 2" >> /etc/fstab
   # mount /data
   ```

2. Mount the new local storage:

   ```
   # mount -a
   ```

3. Ensure that the directory has permissions allowing read/write access to the **vdsm** user (UID 36) and **kvm** group (GID 36):

   ```
   # chown 36:36 /data /rhvh-data
   # chmod 0755 /data /rhvh-data
   ```

5.6. PREPARING RED HAT GLUSTER STORAGE

For information on setting up and configuring Red Hat Gluster Storage, see the *Red Hat Gluster Storage Installation Guide*.

For the Red Hat Gluster Storage versions that are supported with Red Hat Virtualization, see Red Hat Gluster Storage Version Compatibility and Support.

5.7. CUSTOMIZING MULTIPATH CONFIGURATIONS FOR SAN VENDORS

If your RHV environment is configured to use multipath connections with SANs, you can customize the multipath configuration settings to meet requirements specified by your storage vendor. These customizations can override both the default settings and settings that are specified in **/etc/multipath.conf**.

To override the multipath settings, do not customize **/etc/multipath.conf**. Because VDSM owns **/etc/multipath.conf**, installing or upgrading VDSM or Red Hat Virtualization can overwrite this file including any customizations it contains. This overwriting can cause severe storage failures.

Instead, you create a file in the **/etc/multipath/conf.d** directory that contains the settings you want to customize or override.

VDSM executes the files in **/etc/multipath/conf.d** in alphabetical order. So, to control the order of execution, you begin the filename with a number that makes it come last. For example, **/etc/multipath/conf.d/90-myfile.conf**.

To avoid causing severe storage failures, follow these guidelines:

- Do not modify **/etc/multipath.conf**. If the file contains user modifications, and the file is overwritten, it can cause unexpected storage problems.
- Do not override the **user_friendly_names** and **find_multipaths** settings. For details, see Recommended Settings for Multipath.conf.
- Avoid overriding the **no_path_retry** and **polling_interval** settings unless a storage vendor specifically requires you to do so. For details, see Recommended Settings for Multipath.conf.

WARNING

Not following these guidelines can cause catastrophic storage errors.

Prerequisites

- VDSM is configured to use the multipath module. To verify this, enter:

```
# vdsm-tool is-configured --module multipath
```

Procedure

1. Create a new configuration file in the **/etc/multipath/conf.d** directory.
2. Copy the individual setting you want to override from **/etc/multipath.conf** to the new configuration file in **/etc/multipath/conf.d/<my_device>.conf**. Remove any comment marks, edit the setting values, and save your changes.
3. Apply the new configuration settings by entering:

```
# systemctl reload multipathd
```

NOTE

Do not restart the multipathd service. Doing so generates errors in the VDSM logs.

Verification steps

1. Test that the new configuration performs as expected on a non-production cluster in a variety of failure scenarios. For example, disable all of the storage connections.

2. Enable one connection at a time and verify that doing so makes the storage domain reachable.

Additional resources

- Recommended Settings for Multipath.conf
- *Red Hat Enterprise Linux DM Multipath*
- Configuring iSCSI Multipathing
- How do I customize /etc/multipath.conf on my RHVH hypervisors? What values must not change and why?

5.8. RECOMMENDED SETTINGS FOR MULTIPATH.CONF

Do not override the following settings:

user_friendly_names no

Device names must be consistent across all hypervisors. For example, **/dev/mapper/{WWID}**. The default value of this setting, **no**, prevents the assignment of arbitrary and inconsistent device names such as **/dev/mapper/mpath{N}** on various hypervisors, which can lead to unpredictable system behavior.

WARNING

Do not change this setting to **user_friendly_names yes**. User-friendly names are likely to cause unpredictable system behavior or failures, and are not supported.

find_multipaths no

This setting controls whether RHVH tries to access devices through multipath only if more than one path is available. The current value, **no**, allows RHV to access devices through multipath even if only one path is available.

WARNING

Do not override this setting.

Avoid overriding the following settings unless required by the storage system vendor:

no_path_retry 4

This setting controls the number of polling attempts to retry when no paths are available. Before RHV version 4.2, the value of **no_path_retry** was **fail** because QEMU had trouble with the I/O queuing when no paths were available. The **fail** value made it fail quickly and paused the virtual machine. RHV version 4.2 changed this value to **4** so when multipathd detects the last path has failed, it checks all of the paths four more times. Assuming the default 5-second polling interval, checking the paths takes 20 seconds. If no path is up, multipathd tells the kernel to stop queuing and fails all outstanding and future I/O until a path is restored. When a path is restored, the 20-second delay is reset for the next time all paths fail. For more details, see the commit that changed this setting.

polling_interval 5

This setting determines the number of seconds between polling attempts to detect whether a path is open or has failed. Unless the vendor provides a clear reason for increasing the value, keep the VDSM-generated default so the system responds to path failures sooner.

CHAPTER 6. ADDING STORAGE FOR RED HAT VIRTUALIZATION

Add storage as data domains in the new environment. A Red Hat Virtualization environment must have at least one data domain, but adding more is recommended.

Add the storage you prepared earlier:

- NFS
- iSCSI
- Fibre Channel (FCP)
- POSIX-compliant file system
- Local storage
- Red Hat Gluster Storage

6.1. ADDING NFS STORAGE

This procedure shows you how to attach existing NFS storage to your Red Hat Virtualization environment as a data domain.

If you require an ISO or export domain, use this procedure, but select **ISO** or **Export** from the **Domain Function** list.

Procedure

1. In the Administration Portal, click **Storage → Domains**.
2. Click **New Domain**.
3. Enter a **Name** for the storage domain.
4. Accept the default values for the **Data Center**, **Domain Function**, **Storage Type**, **Format**, and **Host** lists.
5. Enter the **Export Path** to be used for the storage domain. The export path should be in the format of *123.123.0.10:/data* (for IPv4), *[2001:0:0:0:0:0:0:5db1]:/data* (for IPv6), or *domain.example.com:/data*.
6. 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

   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.

7. Click **OK**.

The new NFS data domain has a status of **Locked** until the disk is prepared. The data domain is then automatically attached to the data center.

6.2. ADDING ISCSI STORAGE

This procedure shows you how to attach existing iSCSI storage to your Red Hat Virtualization environment as a data domain.

Procedure

1. Click **Storage** → **Domains**.
2. Click **New Domain**.
3. Enter the **Name** of the new storage domain.
4. Select a **Data Center** from the drop-down list.
5. Select **Data** as the **Domain Function** and **iSCSI** as the **Storage Type**.
6. Select an active host as the **Host**.

   IMPORTANT

   Communication to the storage domain is from the selected host and not directly from the Manager. Therefore, all hosts must have access to the storage device before the storage domain can be configured.

7. The Manager can map iSCSI targets to LUNs or LUNs to iSCSI targets. The **New Domain** window automatically displays known targets with unused LUNs when the iSCSI storage type is selected. If the target that you are using to add storage does not appear, you can use target discovery to find it; otherwise proceed to the next step.

   a. Click **Discover Targets** to enable target discovery options. When targets have been discovered and logged in to, the **New Domain** window automatically displays targets with LUNs unused by the environment.

      NOTE

      LUNs used externally for the environment are also displayed.

      You can use the **Discover Targets** options to add LUNs on many targets or multiple paths to the same LUNs.

IMPORTANT

If you use the REST API method **discoveriscsi** to discover the iscsi targets, you can use an FQDN or an IP address, but you must use the iscsi details from the discovered targets results to log in using the REST API method **iscsilogin**. See discoveriscsi in the *REST API Guide* for more information.

b. Enter the FQDN or IP address of the iSCSI host in the **Address** field.

c. Enter the port with which to connect to the host when browsing for targets in the **Port** field. The default is **3260**.

d. If CHAP is used to secure the storage, select the **User Authentication** check box. Enter the **CHAP user name** and **CHAP password**.

NOTE

You can define credentials for an iSCSI target for a specific host with the REST API. See StorageServerConnectionExtensions: add in the *REST API Guide* for more information.

e. Click **Discover**.

f. Select one or more targets from the discovery results and click **Login** for one target or **Login All** for multiple targets.

IMPORTANT

If more than one path access is required, you must discover and log in to the target through all the required paths. Modifying a storage domain to add additional paths is currently not supported.

IMPORTANT

When using the REST API **iscsilogin** method to log in, you must use the iscsi details from the discovered targets results in the **discoveriscsi** method. See iscsilogin in the *REST API Guide* for more information.

8. Click the **+** button next to the desired target. This expands the entry and displays all unused LUNs attached to the target.

9. Select the check box for each LUN that you are using to create the storage domain.

10. 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.

    e. Select the **Discard After Delete** check box to enable the discard after delete option. This option can be edited after the domain is created. This option is only available to block storage domains.

11. Click **OK**.

If you have configured multiple storage connection paths to the same target, follow the procedure in Configuring iSCSI Multipathing to complete iSCSI bonding.

If you want to migrate your current storage network to an iSCSI bond, see Migrating a Logical Network to an iSCSI Bond.

6.3. ADDING FCP STORAGE

This procedure shows you how to attach existing FCP storage to your Red Hat Virtualization environment as a data domain.

Procedure

1. Click **Storage → Domains**.

2. Click **New Domain**.

3. Enter the **Name** of the storage domain.

4. Select an FCP **Data Center** from the drop-down list.
   If you do not yet have an appropriate FCP data center, select **(none)**.

5. Select the **Domain Function** and the **Storage Type** from the drop-down lists. The storage domain types that are not compatible with the chosen data center are not available.

6. Select an active host in the **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 unused LUNs when **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.

e. Select the **Discard After Delete** check box to enable the discard after delete option. This option can be edited after the domain is created. This option is only available to block storage domains.

9. Click **OK**.

The new FCP data domain remains in a **Locked** status while it is being prepared for use. When ready, it is automatically attached to the data center.

6.4. ADDING POSIX-COMPLIANT FILE SYSTEM STORAGE

This procedure shows you how to attach existing POSIX-compliant file system storage to your Red Hat Virtualization environment as a data domain.

Procedure

1. Click **Storage → Domains**.

2. Click **New Domain**.

3. Enter the **Name** for the storage domain.

4. Select the **Data Center** to be associated with the storage domain. The data center selected must be of type **POSIX (POSIX compliant FS)**. Alternatively, select **(none)**.

5. Select **Data** from the **Domain Function** drop-down list, and **POSIX compliant FS** from the **Storage Type** drop-down list.
   If applicable, select the **Format** from the drop-down menu.

6. Select a host from the **Host** drop-down list.

7. Enter the **Path** to the POSIX file system, as you would normally provide it to the **mount** command.

8. Enter the **VFS Type**, as you would normally provide it to the **mount** command using the **-t** argument. See **man mount** for a list of valid VFS types.

9. Enter additional **Mount Options**, as you would normally provide them to the **mount** command using the **-o** argument. The mount options should be provided in a comma-separated list. See **man mount** for a list of valid mount options.

10. Optionally, you can configure the advanced parameters.

    a. Click **Advanced Parameters**.

   b. Enter a percentage value in 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 in 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.

11. Click **OK**.

6.5. ADDING A LOCAL STORAGE DOMAIN

When adding a local storage domain to a host, setting the path to the local storage directory automatically creates and places the host in a local data center, local cluster, and local storage domain.

Procedure

1. Click **Compute → Hosts** and select the host.
2. Click **Management → Maintenance** and **OK**. The host's status changes to **Maintenance**.
3. Click **Management → Configure Local Storage**.
4. Click the **Edit** buttons next to the **Data Center**, **Cluster**, and **Storage** fields to configure and name the local storage domain.
5. Set the path to your local storage in the text entry field.
6. If applicable, click the **Optimization** tab to configure the memory optimization policy for the new local storage cluster.
7. Click **OK**.

The Manager sets up the local data center with a local cluster, local storage domain. It also changes the host's status to **Up**.

Verification

1. Click **Storage → Domains**.
2. Locate the local storage domain you just added.

The domain's status should be **Active** (▲), and the value in the **Storage Type** column should be **Local on Host**.

You can now upload a disk image in the new local storage domain.

6.6. ADDING RED HAT GLUSTER STORAGE

To use Red Hat Gluster Storage with Red Hat Virtualization, see *Configuring Red Hat Virtualization with Red Hat Gluster Storage*.

For the Red Hat Gluster Storage versions that are supported with Red Hat Virtualization, see Red Hat Gluster Storage Version Compatibility and Support.

APPENDIX A. 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.

Prerequisites

- A Red Hat Enterprise Linux 8 Server installed on a system that has access to the Content Delivery Network. This system downloads all the required packages, and distributes them to your offline systems.
- 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.

Begin by enabling the Red Hat Virtualization Manager repositories on the online system:

Enabling the Red Hat Virtualization Manager Repositories

You need to log in and register the online machine with Red Hat Subscription Manager, attach the **Red Hat Virtualization Manager** subscription, 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
```

NOTE

If you are using an IPv6 network, use an IPv6 transition mechanism to access the Content Delivery Network and subscription manager.

2. Find the **Red Hat Virtualization Manager** subscription pool and record the pool ID:

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

3. Use the pool ID to attach the subscription to the system:

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

NOTE

To view currently attached subscriptions:

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

To list all enabled repositories:

```
# dnf repolist
```

4. Configure the repositories:

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-8-for-x86_64-baseos-eus-rpms \
    --enable=rhel-8-for-x86_64-appstream-eus-rpms \
    --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
    --enable=fast-datapath-for-rhel-8-x86_64-rpms \
    --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
    --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
    --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
    --enable=rhel-8-for-x86_64-appstream-tus-rpms \
    --enable=rhel-8-for-x86_64-baseos-tus-rpms
```

5. Set the RHEL version to 8.6:

```
# subscription-manager release --set=8.6
```

6. Enable the **pki-deps** module.

```
# dnf module -y enable pki-deps
```

7. Enable version 12 of the **postgresql** module.

```
# dnf module -y enable postgresql:12
```

8. Enable version 14 of the **nodejs** module:

```
# dnf module -y enable nodejs:14
```

9. Synchronize installed packages to update them to the latest available versions.

```
# dnf distro-sync --nobest
```

Additional resources

For information on modules and module streams, see the following sections in *Installing, managing, and removing user-space components*

- Module streams
- Selecting a stream before installation of packages

- Resetting module streams
- Switching to a later stream

Configuring the Offline Repository

1. 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** on the intended Manager machine:

   a. Install the **vsftpd** package:

   ```
   # dnf install vsftpd
   ```

   b. Enable ftp access for an anonymous user to have access to rpm files from the intended Manager machine, and to keep it secure, disable write on ftp server. Edit the **/etc/vsftpd/vsftpd.conf** file and change the values for **anonymous_enable** and **write_enable** as follows:

   ```
   anonymous_enable=YES
   write_enable=NO
   ```

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

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

   d. Create a firewall rule to allow FTP service and reload the **firewalld** service to apply changes:

   ```
   # firewall-cmd --permanent --add-service=ftp
   # firewall-cmd --reload
   ```

   e. Red Hat Enterprise Linux 8 enforces SELinux by default, so configure SELinux to allow FTP access:

   ```
   # setsebool -P allow_ftpd_full_access=1
   ```

   f. Create a sub-directory inside the **/var/ftp/pub/** directory, where the downloaded packages are made available:

   ```
   # mkdir /var/ftp/pub/rhvrepo
   ```

2. Download packages from all configured software repositories to the **rhvrepo** directory. This includes repositories for all Content Delivery Network subscription pools attached to the system, and any locally configured repositories:

   ```
   # reposync -p /var/ftp/pub/rhvrepo --download-metadata
   ```

   This command downloads a large number of packages and their metadata, and takes a long time to complete.

3. Create a repository file, and copy it to the **/etc/yum.repos.d/** directory on the intended Manager machine.

You can create the configuration file manually or with a script. Run the script below on the machine hosting the repository, replacing *ADDRESS* in the **baseurl** with the IP address or FQDN of the machine hosting the repository:

```
#!/bin/sh

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

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

Return to Configuring the Manager. Packages are installed from the local repository, instead of from the Content Delivery Network.

Troubleshooting

When running **reposync**, the following error message appears

No available modular metadata for modular package "package_name_from_module" it cannot be installed on the system

Solution

Ensure you have **yum-utils-4.0.8-3.el8.noarch** or higher installed so reposync correctly downloads all the packages. For more information, see Create a local repo with Red Hat Enterprise Linux 8 .

APPENDIX B. CONFIGURING A HOST FOR PCI PASSTHROUGH

NOTE

This is one in a series of topics that show how to set up and configure SR-IOV on Red Hat Virtualization. For more information, see Setting Up and Configuring SR-IOV

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 must 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 first.

Prerequisites

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

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 Deployment 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 Standard Hosts to the Red Hat Virtualization Manager and Kernel Settings Explained.

   - To edit the **grub** configuration file manually, see Enabling IOMMU Manually.

3. For GPU passthrough, you need to run additional configuration steps on both the host and the guest system. See GPU device passthrough: Assigning a host GPU to a single virtual machine in *Setting up an NVIDIA GPU for a virtual machine in Red Hat Virtualization* for more information.

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 an AMD IOMMU is detected, you can try adding **iommu=pt**. The **pt** option only enables IOMMU for devices used in passthrough and provides better host performance. However, the option might not be supported on all hardware. Revert to the 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
```

APPENDIX C. REMOVING THE STANDALONE RED HAT VIRTUALIZATION MANAGER

The **engine-cleanup** command removes all components of the Red Hat Virtualization Manager and automatically backs up the following:

- the Grafana database, in **/var/lib/grafana/**
- the Manager database in **/var/lib/ovirt-engine/backups/**
- a compressed archive of the PKI keys and configuration in **/var/lib/ovirt-engine/backups/**

Backup file names include the date and time.

> **WARNING**
>
> You should use this procedure only on a standalone installation of the Red Hat Virtualization Manager.

Procedure

1. Run the following command on the Manager machine:

   ```
   # engine-cleanup
   ```

2. The Manager service must be stopped before proceeding. You are prompted to confirm. Enter **OK** to proceed:

   ```
   During execution engine service will be stopped (OK, Cancel) [OK]:
   ```

3. You are prompted to confirm that you want to remove all Manager components. Enter **OK** to remove all components, or **Cancel** to exit **engine-cleanup**:

   ```
   All the installed ovirt components are about to be removed, data will be lost (OK, Cancel)
   [Cancel]: OK
   ```

   engine-cleanup details the components that are removed, and the location of backup files.

4. Remove the Red Hat Virtualization packages:

   ```
   # dnf remove rhvm* vdsm-bootstrap
   ```

APPENDIX D. PREVENTING KERNEL MODULES FROM LOADING AUTOMATICALLY

You can prevent a kernel module from being loaded automatically, whether the module is loaded directly, loaded as a dependency from another module, or during the boot process.

Procedure

1. The module name must be added to a configuration file for the **modprobe** utility. This file must reside in the configuration directory **/etc/modprobe.d**.
   For more information on this configuration directory, see the man page **modprobe.d**.

2. Ensure the module is not configured to get loaded in any of the following:

   - **/etc/modprobe.conf**
   - **/etc/modprobe.d/***
   - **/etc/rc.modules**
   - **/etc/sysconfig/modules/***

   ```
   # modprobe --showconfig <_configuration_file_name_>
   ```

3. If the module appears in the output, ensure it is ignored and not loaded:

   ```
   # modprobe --ignore-install <_module_name_>
   ```

4. Unload the module from the running system, if it is loaded:

   ```
   # modprobe -r <_module_name_>
   ```

5. Prevent the module from being loaded directly by adding the **blacklist** line to a configuration file specific to the system - for example **/etc/modprobe.d/local-dontload.conf**:

   ```
   # echo "blacklist <_module_name_> >> /etc/modprobe.d/local-dontload.conf
   ```

   NOTE

   This step does not prevent a module from loading if it is a required or an optional dependency of another module.

6. Prevent optional modules from being loading on demand:

   ```
   # echo "install <_module_name_>/bin/false" >> /etc/modprobe.d/local-dontload.conf
   ```

   IMPORTANT

   If the excluded module is required for other hardware, excluding it might cause unexpected side effects.

7. Make a backup copy of your **initramfs**:

   ```
   # cp /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.$(date +%m-%d-
   %H%M%S).bak
   ```

8. If the kernel module is part of the **initramfs**, rebuild your initial **ramdisk** image, omitting the module:

   ```
   # dracut --omit-drivers <_module_name_> -f
   ```

9. Get the current kernel command line parameters:

   ```
   # grub2-editenv - list | grep kernelopts
   ```

10. Append **<_module_name_>.blacklist=1 rd.driver.blacklist=<_module_name_>** to the generated output:

    ```
    # grub2-editenv - set kernelopts="<> <_module_name_>.blacklist=1 rd.driver.blacklist=
    <_module_name_>"
    ```

    For example:

    ```
    # grub2-editenv - set kernelopts="root=/dev/mapper/rhel_example-root ro crashkernel=auto
    resume=/dev/mapper/rhel_example-swap rd.lvm.lv=rhel_example/root
    rd.lvm.lv=rhel_example/swap <_module_name_>.blacklist=1 rd.driver.blacklist=
    <_module_name_>"
    ```

11. Make a backup copy of the **kdump initramfs**:

    ```
    # cp /boot/initramfs-$(uname -r)kdump.img /boot/initramfs-$(uname -r)kdump.img.$(date
    +%m-%d-%H%M%S).bak
    ```

12. Append **rd.driver.blacklist=<_module_name_>** to the **KDUMP_COMMANDLINE_APPEND** setting in **/etc/sysconfig/kdump** to omit it from the **kdump initramfs**:

    ```
    # sed -i '/^KDUMP_COMMANDLINE_APPEND=/s/"$/ rd.driver.blacklist=module_name"/'
    /etc/sysconfig/kdump
    ```

13. Restart the **kdump** service to pick up the changes to the **kdump initrd**:

    ```
     # kdumpctl restart
    ```

14. Rebuild the **kdump** initial **ramdisk** image:

    ```
     # mkdumprd -f /boot/initramfs-$(uname -r)kdump.img
    ```

15. Reboot the system.

D.1. REMOVING A MODULE TEMPORARILY

You can remove a module temporarily.

Procedure

1. Run **modprobe** to remove any currently-loaded module:

   ```
   # modprobe -r <module name>
   ```

2. If the module cannot be unloaded, a process or another module might still be using the module. If so, terminate the process and run the **modpole** command written above another time to unload the module.

APPENDIX E. SECURING RED HAT VIRTUALIZATION

This information is specific to Red Hat Virtualization. It does not cover fundamental security practices related to any of the following:

- Disabling unnecessary services
- Authentication
- Authorization
- Accounting
- Penetration testing and hardening of non-RHV services
- Encryption of sensitive application data

Prerequisites

- You should be proficient in your organization’s security standards and practices. If possible, consult with your organization’s Security Officer.
- Consult the Red Hat Enterprise Linux Security hardening before deploying RHEL hosts.

E.1. APPLYING THE DISA STIG PROFILE IN RHEL BASED HOSTS AND THE STANDALONE MANAGER

When installing RHV, you can select the DISA STIG profile with the UI installer, which is the profile provided by RHEL 8.

IMPORTANT

The DISA STIG profile is not supported for Red Hat Virtualization Host (RHVH).

Procedure

1. In the **Installation Summary** screen, select **Security Policy**.
2. In the **Security Policy** screen, set the **Apply security policy** to **On**.
3. Select **DISA STIG for Red Hat Enterprise Linux 8**
4. Click **Select profile**. This action adds a green checkmark next to the profile and adds packages to the list of **Changes that were done or need to be done** Follow the onscreen instructions if they direct you to make any changes.
5. Click **Done**.
6. On the **Installation Summary** screen, verify that the status of **Security Policy** is **Everything okay**.
7. Reboot the host.

E.1.1. Enabling DISA STIG in a self-hosted engine

You can enable DISA STIG in a self-hosted engine during deployment when using the command-line.

Procedure

1. Start the self-hosted engine deployment script. See Installing Red Hat Virtualization as a self-hosted engine using the command line.
2. When the deployment script prompts **Do you want to apply an OpenSCAP security profile?**, enter **Yes**.
3. When the deployment script prompts **Please provide the security profile you would like to use?**, enter **stig**.

E.2. APPLYING THE PCI-DSS PROFILE IN RHV HOSTS AND THE STANDALONE MANAGER

When installing RHVH, you can select the PCI-DSS profile with the UI installer, which is the profile provided by RHEL 8.

Procedure

1. In the **Installation Summary** screen, select **Security Policy**.
2. In the **Security Policy** screen, set the **Apply security policy** to **On**.
3. Select **PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8**
4. Click **Select profile**. This action adds a green checkmark next to the profile and adds packages to the list of **Changes that were done or need to be done** Follow the onscreen instructions if they direct you to make any changes.
5. Click **Done**.
6. In the **Installation Summary** screen, verify that the status of **Security Policy** is **Everything okay**.
7. Reboot the host.

E.2.1. Enabling PCI-DSS in a self-hosted engine

You can enable PCI-DSS in a self-hosted engine during deployment when using the command-line.

Procedure

1. Start the self-hosted engine deployment script. See Installing Red Hat Virtualization as a self-hosted engine using the command line.
2. When the deployment script prompts **Do you want to apply an OpenSCAP security profile?**, enter **Yes**.
3. When the deployment script prompts **Please provide the security profile you would like to use?**, enter **pci-dss**.

APPENDIX F. LEGAL NOTICE