Red Hat Virtualization 4.4

Planning and Prerequisites Guide

Planning the installation and configuration of Red Hat Virtualization 4.4

Last Updated: 2020-09-23

Red Hat Virtualization 4.4 Planning and Prerequisites Guide

Planning the installation and configuration of Red Hat Virtualization 4.4

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

Legal Notice

Abstract

This document provides requirements, options, and recommendations for Red Hat Virtualization environments.

Table of Contents

PREFACE 4

CHAPTER 1. RED HAT VIRTUALIZATION ARCHITECTURE 5
1.1. SELF-HOSTED ENGINE ARCHITECTURE 5
1.2. STANDALONE MANAGER ARCHITECTURE 5

CHAPTER 2. REQUIREMENTS 7
2.1. RED HAT VIRTUALIZATION MANAGER REQUIREMENTS 7
2.1.1. Hardware Requirements 7
2.1.2. Browser Requirements 7
2.1.3. Client Requirements 8
2.1.4. Operating System Requirements 8
2.2. HOST REQUIREMENTS 9
2.2.1. CPU Requirements 9
2.2.1.1. Checking if a Processor Supports the Required Flags 10
2.2.2. Memory Requirements 10
2.2.3. Storage Requirements 10
2.2.4. PCI Device Requirements 11
2.2.5. Device Assignment Requirements 11
2.2.6. vGPU Requirements 12
2.3. NETWORKING REQUIREMENTS 12
2.3.1. General requirements 12
2.3.2. Network range for self-hosted engine deployment 12
2.3.3. Firewall Requirements for DNS, NTP, and IPMI Fencing 12
2.3.4. Red Hat Virtualization Manager Firewall Requirements 13
2.3.5. Host Firewall Requirements 16
2.3.6. Database Server Firewall Requirements 20

CHAPTER 3. CONSIDERATIONS 22
3.1. HOST TYPES 22
3.1.1. Red Hat Virtualization Hosts 22
3.1.2. Red Hat Enterprise Linux hosts 22
3.2. STORAGE TYPES 22
3.2.1. NFS 23
3.2.2. iSCSI 23
3.2.3. Fibre Channel over Ethernet 24
3.2.4. Red Hat Gluster Storage 24
3.2.5. Red Hat Hyperconverged Infrastructure 24
3.2.6. POSIX-Compliant FS 24
3.2.7. Local Storage 25
3.3. NETWORKING CONSIDERATIONS 25
3.4. DIRECTORY SERVER SUPPORT 26
3.5. INFRASTRUCTURE CONSIDERATIONS 26
3.5.1. Local or Remote Hosting 27
3.5.2. Remote Hosting Only 27

CHAPTER 4. RECOMMENDATIONS 29
4.1. GENERAL RECOMMENDATIONS 29
4.2. SECURITY RECOMMENDATIONS 29
4.3. HOST RECOMMENDATIONS 30
4.4. NETWORKING RECOMMENDATIONS 30
Recommended Practices for Configuring Host Networks 31

4.5. SELF-HOSTED ENGINE RECOMMENDATIONS 32

PREFACE

Red Hat Virtualization is made up of connected components that each play different roles in the environment. Planning and preparing for their requirements in advance helps these components communicate and run efficiently.

This guide covers:

- Hardware and security requirements
- The options available for various components
- Recommendations for optimizing your environment

CHAPTER 1. RED HAT VIRTUALIZATION ARCHITECTURE

Red Hat Virtualization can be deployed as a self-hosted engine, or as a standalone Manager. A self-hosted engine is the recommended deployment option.

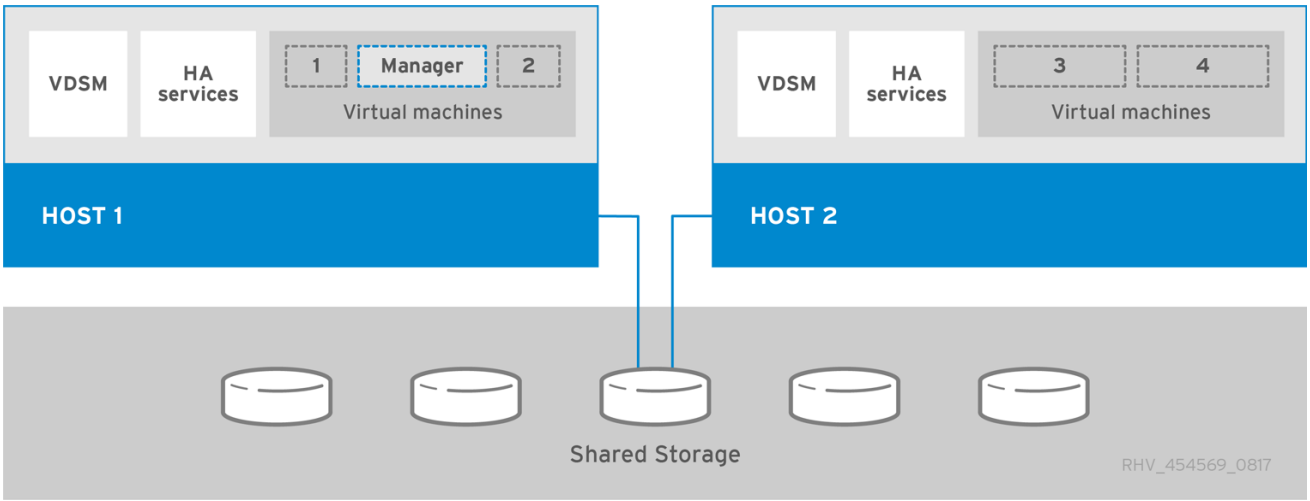
1.1. SELF-HOSTED ENGINE ARCHITECTURE

The Red Hat Virtualization Manager runs as a virtual machine on self-hosted engine nodes (specialized hosts) in the same environment it manages. A self-hosted engine environment requires one less physical server, but requires more administrative overhead to deploy and manage. The Manager is highly available without external HA management.

The minimum setup of a self-hosted engine environment includes:

- One Red Hat Virtualization Manager virtual machine that is hosted on the self-hosted engine nodes. The RHV-M Appliance is used to automate the installation of a Red Hat Enterprise Linux 8 virtual machine, and the Manager on that virtual machine.
- A minimum of two self-hosted engine nodes 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. The HA services run on all self-hosted engine nodes to manage the high availability of the Manager virtual machine.
- 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 1.1. Self-Hosted Engine Red Hat Virtualization Architecture



1.2. STANDALONE MANAGER ARCHITECTURE

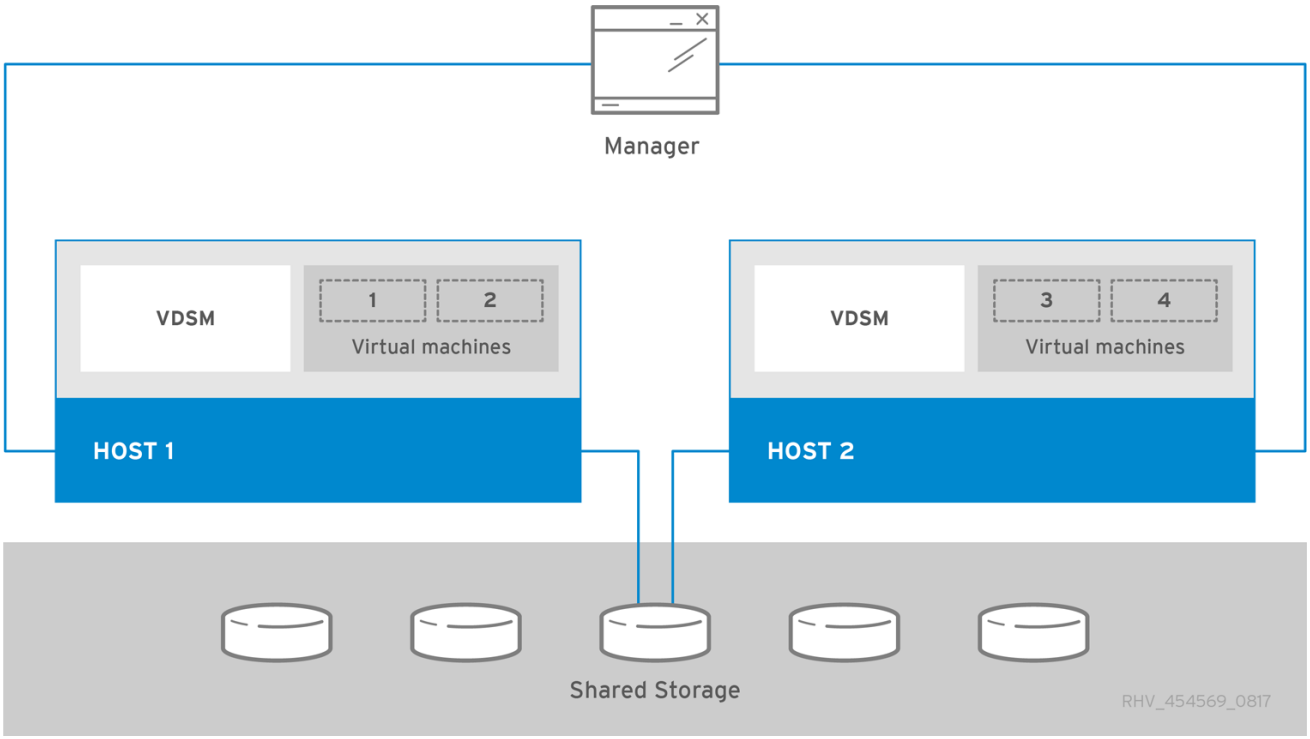
The Red Hat Virtualization Manager runs on a physical server, or a virtual machine hosted in a separate virtualization environment. A standalone Manager is easier to deploy and manage, but requires an additional physical server. The Manager is only highly available when managed externally with a product 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 1.2. Standalone Manager Red Hat Virtualization Architecture



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 https://access.redhat.com/solutions/725243. To confirm whether specific hardware items are certified for use with Red Hat Enterprise Linux, see https://access.redhat.com/ecosystem/#certifiedHardware.

Table 2.1. Red Hat Virtualization Manager Hardware Requirements

Resource	Minimum	Recommended
CPU	A dual core CPU.	A quad core CPU or multiple dual core CPUs.
Memory	4 GB of available system RAM if Data Warehouse is not installed and if memory is not being consumed by existing processes.	16 GB of system RAM.
Hard Disk	25 GB of locally accessible, writable disk space.	50 GB of locally accessible, writable disk space. You can use the 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

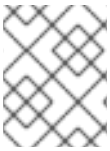
2.1.3. Client Requirements

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 that has been updated to the latest minor release.

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 https://access.redhat.com/solutions/725243. To confirm whether specific hardware items are certified for use with Red Hat Enterprise Linux, see https://access.redhat.com/ecosystem/#certifiedHardware.

For more information on the requirements and limitations that apply to guests see https://access.redhat.com/articles/rhel-limits and https://access.redhat.com/articles/906543.

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.

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. The maximum supported RAM per VM in Red Hat Virtualization Host is 4 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 - 15 GB
- /var/crash - 10 GB
- /var/log - 8 GB
- /var/log/audit - 2 GB
- swap - 1 GB (for the recommended swap size, see https://access.redhat.com/solutions/15244)
- 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 5 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
- Predefined **mdev_type** set to correspond with one of the mdev types supported by the device
- 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. Network range for self-hosted engine deployment

The self-hosted engine deployment process temporarily uses a **/24** network address under **192.168**. It defaults to **192.168.222.0/24**, and if this address is in use, it tries other **/24** addresses under **192.168** until it finds one that is not in use. If it does not find an unused network address in this range, deployment fails.

When installing the self-hosted engine using the command line, you can set the deployment script to use an alternate **/24** network range with the option **--ansible-extra-vars=he_ipv4_subnet_prefix=*PREFIX***, where ***PREFIX*** is the prefix for the default range. For example:

```
# hosted-engine --deploy --ansible-extra-vars=he_ipv4_subnet_prefix=192.168.222
```

NOTE

You can only set another range by installing Red Hat Virtualization as a self-hosted engine using the command line.

2.3.3. 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.

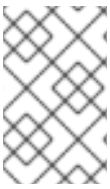
The firewall requirement tables in the following sections do not represent this option.

2.3.4. 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

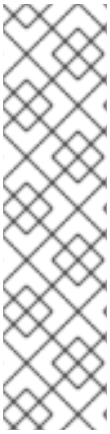
A diagram of these firewall requirements is available at https://access.redhat.com/articles/3932211. You can use the IDs in the table to look up connections in the diagram.

Table 2.3. Red Hat Virtualization Manager Firewall Requirements

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
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
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. If the websocket proxy is running on a different host, however, this port is not used.	No

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
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 (ImageIO Proxy server)	Required for communication with the ImageIO Proxy (**ovirt-imageio-proxy**).	Yes
M8	6442	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

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

2.3.5. 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 https://access.redhat.com/solutions/2772331.

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 2.4. Virtualization Host Firewall Requirements

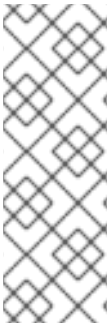
ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
H1	22	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Secure Shell (SSH) access. Optional.	Yes

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

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

ID	Port(s)	Protocol	Source	Destination	Purpose	Encrypted by default
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
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 (ImageIO Proxy server)	Red Hat Virtualization Hosts Red Hat Enterprise Linux hosts	Required for communication with the ImageIO daemon (**ovirt-imageio-daemon**).	Yes

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



NOTE

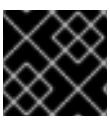
By default, Red Hat Enterprise Linux allows outbound traffic to DNS and NTP on any destination address. If you disable outgoing traffic, make exceptions for the Red Hat Virtualization Hosts

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.

2.3.6. Database Server Firewall Requirements

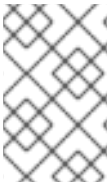
Red Hat Virtualization supports the use of a remote database server for the Manager database (**engine**) and the Data Warehouse database (**ovirt-engine-history**). If you plan to use a remote database server, it must allow connections from the Manager and the Data Warehouse service (which can be separate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

CHAPTER 3. CONSIDERATIONS

This chapter describes the advantages, limitations, and available options for various Red Hat Virtualization components.

3.1. HOST TYPES

Use the host type that best suits your environment. You can also use both types of host in the same cluster if required.

All managed hosts within a cluster must have the same CPU type. Intel and AMD CPUs cannot co-exist within the same cluster.

For information about supported maximums and limits, such as the maximum number of hosts that the Red Hat Virtualization Manager can support, see Supported Limits for Red Hat Virtualization .

3.1.1. Red Hat Virtualization Hosts

Red Hat Virtualization Hosts (RHVH) have the following advantages over Red Hat Enterprise Linux hosts:

- RHVH is included in the subscription for Red Hat Virtualization. Red Hat Enterprise Linux hosts may require additional subscriptions.
- RHVH is deployed as a single image. This results in a streamlined update process; the entire image is updated as a whole, as opposed to packages being updated individually.
- Only the packages and services needed to host virtual machines or manage the host itself are included. This streamlines operations and reduces the overall attack vector; unnecessary packages and services are not deployed and, therefore, cannot be exploited.
- The Cockpit web interface is available by default and includes extensions specific to Red Hat Virtualization, including virtual machine monitoring tools and a GUI installer for the self-hosted engine. Cockpit is supported on Red Hat Enterprise Linux hosts, but must be manually installed.

3.1.2. Red Hat Enterprise Linux hosts

Red Hat Enterprise Linux hosts have the following advantages over Red Hat Virtualization Hosts:

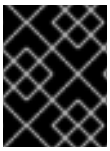
- Red Hat Enterprise Linux hosts are highly customizable, so may be preferable if, for example, your hosts require a specific file system layout.
- Red Hat Enterprise Linux hosts are better suited for frequent updates, especially if additional packages are installed. Individual packages can be updated, rather than a whole image.

3.2. STORAGE TYPES

Each data center must have at least one data storage domain. An ISO storage domain per data center is also recommended. Export storage domains are deprecated, but can still be created if necessary.

A storage domain can be made of either block devices (iSCSI or Fibre Channel) or a file system.

By default, GlusterFS domains and local storage domains support 4K block size. 4K block size can provide better performance, especially when using large files, and it is also necessary when you use tools that require 4K compatibility, such as VDO.



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.

The storage types described in the following sections are supported for use as data storage domains. ISO and export storage domains only support file-based storage types. The ISO domain supports local storage when used in a local storage data center.

See:

- Storage in the *Administration Guide*.
- *Red Hat Enterprise Linux Storage Administration Guide*

3.2.1. NFS

NFS versions 3 and 4 are supported by Red Hat Virtualization 4. Production workloads require an enterprise-grade NFS server, unless NFS is only being used as an ISO storage domain. When enterprise NFS is deployed over 10GbE, segregated with VLANs, and individual services are configured to use specific ports, it is both fast and secure.

As NFS exports are grown to accommodate more storage needs, Red Hat Virtualization recognizes the larger data store immediately. No additional configuration is necessary on the hosts or from within Red Hat Virtualization. This provides NFS a slight edge over block storage from a scale and operational perspective.

See:

- Network File System (NFS) in the *Red Hat Enterprise Linux Storage Administration Guide* .
- Preparing and Adding NFS Storage in the *Administration Guide*.

3.2.2. iSCSI

Production workloads require an enterprise-grade iSCSI server. When enterprise iSCSI is deployed over 10GbE, segregated with VLANs, and utilizes CHAP authentication, it is both fast and secure. iSCSI can also use multipathing to improve high availability.

Red Hat Virtualization supports 1500 logical volumes per block-based storage domain. No more than 300 LUNs are permitted.

See:

- Online Storage Management in the *Red Hat Enterprise Linux Storage Administration Guide* .
- Adding iSCSI Storage in the *Administration Guide*. ==== Fibre Channel

Fibre Channel is both fast and secure, and should be taken advantage of if it is already in use in the target data center. It also has the advantage of low CPU overhead as compared to iSCSI and NFS. Fibre Channel can also use multipathing to improve high availability.

Red Hat Virtualization supports 1500 logical volumes per block-based storage domain. No more than 300 LUNs are permitted.

See:

- Online Storage Management in the *Red Hat Enterprise Linux Storage Administration Guide* .
- Adding FCP Storage in the *Administration Guide*.

3.2.3. Fibre Channel over Ethernet

To use Fibre Channel over Ethernet (FCoE) in Red Hat Virtualization, you must enable the **fcoe** key on the Manager, and install the *vdsm-hook-fcoe* package on the hosts.

Red Hat Virtualization supports 1500 logical volumes per block-based storage domain. No more than 300 LUNs are permitted.

See:

- Online Storage Management in the *Red Hat Enterprise Linux Storage Administration Guide* .
- How to Set Up Red Hat Virtualization Manager to Use FCoE in the *Administration Guide*.

3.2.4. Red Hat Gluster Storage

Red Hat Gluster Storage (RHGS) is a POSIX-compliant and open source file system. Three or more servers are configured as a Red Hat Gluster Storage cluster, instead of network-attached storage (NAS) appliances or a storage area network (SAN) array.

Red Hat Gluster Storage should be utilized over 10GbE and segregated with VLANs.

Check the compatibility matrix in https://access.redhat.com/articles/2356261 before using RHGS with Red Hat Virtualization.

See:

- Red Hat Gluster Storage Documentation
- *Configuring Red Hat Virtualization with Red Hat Gluster Storage*

3.2.5. Red Hat Hyperconverged Infrastructure

Red Hat Hyperconverged Infrastructure (RHHI) combines Red Hat Virtualization and Red Hat Gluster Storage on the same infrastructure, instead of connecting Red Hat Virtualization to a remote Red Hat Gluster Storage server. This compact option reduces operational expenses and overhead.

See:

- *Deploying Red Hat Hyperconverged Infrastructure for Virtualization*
- *Deploying Red Hat Hyperconverged Infrastructure for Virtualization On A Single Node*
- *Automating RHHI for Virtualization Deployment*

3.2.6. POSIX-Compliant FS

Other POSIX-compliant file systems can be used as storage domains in Red Hat Virtualization, as long as they are clustered file systems, such as Red Hat Global File System 2 (GFS2), and 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.

See:

- *Red Hat Enterprise Linux Global File System 2*
- Adding POSIX Compliant File System Storage in the *Administration Guide*.

3.2.7. Local Storage

Local storage is set up on an individual host, using the host's own resources. When you set up a host to use local storage, it is automatically added to a new data center and cluster that no other hosts can be added to. Virtual machines created in a single-host cluster cannot be migrated, fenced, or scheduled.

For Red Hat Virtualization Hosts, local storage should always be defined on a file system that is separate from / (root). Use a separate logical volume or disk.

See: Preparing and Adding Local Storage in the *Administration Guide*.

3.3. NETWORKING CONSIDERATIONS

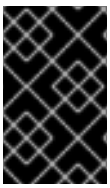
Familiarity with network concepts and their use is highly recommended when planning and setting up networking in a Red Hat Virtualization environment. Read your network hardware vendor's guides for more information on managing networking.

Logical networks may be supported using physical devices such as NICs, or logical devices such as network bonds. Bonding improves high availability, and provides increased fault tolerance, because all network interface cards in the bond must fail for the bond itself to fail. Bonding modes 1, 2, 3, and 4 support both virtual machine and non-virtual machine network types. Modes 0, 5, and 6 only support non-virtual machine networks. Red Hat Virtualization uses Mode 4 by default.

It is not necessary to have one device for each logical network, as multiple logical networks can share a single device by using Virtual LAN (VLAN) tagging to isolate network traffic. To make use of this feature, VLAN tagging must also be supported at the switch level.

The limits that apply to the number of logical networks that you may define in a Red Hat Virtualization environment are:

- The number of logical networks attached to a host is limited to the number of available network devices combined with the maximum number of Virtual LANs (VLANs), which is 4096.
- The number of networks that can be attached to a host in a single operation is currently limited to 50.
- The number of logical networks in a cluster is limited to the number of logical networks that can be attached to a host as networking must be the same for all hosts in a cluster.
- The number of logical networks in a data center is limited only by the number of clusters it contains in combination with the number of logical networks permitted per cluster.



IMPORTANT

Take additional care when modifying the properties of the Management network (**ovirtmgmt**). Incorrect changes to the properties of the **ovirtmgmt** network may cause hosts to become unreachable.

IMPORTANT

If you plan to use Red Hat Virtualization to provide services for other environments, remember that the services will stop if the Red Hat Virtualization environment stops operating.

Red Hat Virtualization is fully integrated with Cisco Application Centric Infrastructure (ACI), which provides comprehensive network management capabilities, thus mitigating the need to manually configure the Red Hat Virtualization networking infrastructure. The integration is performed by configuring Red Hat Virtualization on Cisco's Application Policy Infrastructure Controller (APIC) version 3.1(1) and later, according to the Cisco's documentation.

3.4. DIRECTORY SERVER SUPPORT

During installation, Red Hat Virtualization Manager creates a default **admin** user in a default **internal** domain. This account is intended for use when initially configuring the environment, and for troubleshooting. You can create additional users on the **internal** domain using **ovirt-aaa-jdbc-tool**. User accounts created on local domains are known as local users. See Administering User Tasks From the Command Line in the *Administration Guide*.

You can also attach an external directory server to your Red Hat Virtualization environment and use it as an external domain. User accounts created on external domains are known as directory users. Attachment of more than one directory server to the Manager is also supported.

The following directory servers are supported for use with Red Hat Virtualization. For more detailed information on installing and configuring a supported directory server, see the vendor's documentation.

Active Directory

https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access

Identity Management (IdM - based on IPA)

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.ht

Red Hat Directory Server 9 (RHDS 9 - based on 389DS)

https://access.redhat.com/documentation/en-us/red-hat-directory-server/

OpenLDAP

http://www.openldap.org/doc/

IBM Security (Tivoli) Directory Server

https://www.ibm.com/support/knowledgecenter/SSVJJU_6.4.0/com.ibm.IBMDS.doc_6.4/welcome.ht

IMPORTANT

A user with permissions to read all users and groups must be created in the directory server specifically for use as the Red Hat Virtualization administrative user. Do **not** use the administrative user for the directory server as the Red Hat Virtualization administrative user.

See: Users and Roles in the *Administration Guide*.

3.5. INFRASTRUCTURE CONSIDERATIONS

3.5.1. Local or Remote Hosting

The following components can be hosted on either the Manager or a remote machine. Keeping all components on the Manager machine is easier and requires less maintenance, so is preferable when performance is not an issue. Moving components to a remote machine requires more maintenance, but can improve the performance of both the Manager and Data Warehouse.

Data Warehouse database and service

To host Data Warehouse on the Manager, select **Yes** when prompted by **engine-setup**.
To host Data Warehouse on a remote machine, select **No** when prompted by **engine-setup**, and see Installing and Configuring Data Warehouse on a Separate Machine in *Installing Red Hat Virtualization as a standalone Manager with remote databases*.

To migrate Data Warehouse post-installation, see Migrating Data Warehouse to a Separate Machine in the *Data Warehouse Guide*.

You can also host the Data Warehouse service and the Data Warehouse database separately from one another.

Manager database

To host the Manager database on the Manager, select **Local** when prompted by **engine-setup**.
To host the Manager database on a remote machine, see Preparing a Remote PostgreSQL Database in *Installing Red Hat Virtualization as a standalone Manager with remote databases* before running **engine-setup** on the Manager.

To migrate the Manager database post-installation, see Migrating the Engine Database to a Remote Server Database in the *Administration Guide*.

Websocket proxy

To host the websocket proxy on the Manager, select **Yes** when prompted by **engine-setup**.
To host the websocket proxy on a remote machine, select **No** when prompted by **engine-setup**, and see Installing a Websocket Proxy on a Separate Machine in the *Installing Red Hat Virtualization as a standalone Manager with remote databases*.

IMPORTANT

Self-hosted engine environments use an appliance to install and configure the Manager virtual machine, so Data Warehouse, the Manager database, and the websocket proxy can only be made external post-installation.

3.5.2. Remote Hosting Only

The following components must be hosted on a remote machine:

DNS

Due to the extensive use of DNS in a Red Hat Virtualization environment, running the environment's DNS service as a virtual machine hosted in the environment is not supported.

Storage

With the exception of local storage, the storage service must not be on the same machine as the Manager or any host.

Identity Management

IdM (**ipa-server**) is incompatible with the **mod_ssl** package, which is required by the Manager.

CHAPTER 4. RECOMMENDATIONS

This chapter describes configuration that is not strictly required, but may improve the performance or stability of your environment.

4.1. GENERAL RECOMMENDATIONS

- Take a full backup as soon as the deployment is complete, and store it in a separate location. Take regular backups thereafter. See Backups and Migration in the *Administration Guide*.
- Avoid running any service that Red Hat Virtualization depends on as a virtual machine in the same environment. If this is done, it must be planned carefully to minimize downtime, if the virtual machine containing that service incurs downtime.
- Ensure the bare-metal host or virtual machine that the Red Hat Virtualization Manager will be installed on has enough entropy. Values below 200 can cause the Manager setup to fail. To check the entropy value, run **cat /proc/sys/kernel/random/entropy_avail**. To increase entropy, install the **rng-tools** package and follow the steps in https://access.redhat.com/solutions/1395493.
- You can automate the deployment of hosts and virtual machines using PXE, Kickstart, Satellite, CloudForms, Ansible, or a combination thereof. However, installing a self-hosted engine using PXE is not supported. See:
  - Automating Red Hat Virtualization Host Deployment for the additional requirements for automated RHVH deployment using PXE and Kickstart.
  - Preparing for a Network Installation in the *Red Hat Enterprise Linux 7 Installation Guide* .
  - Kickstart Installations in the *Red Hat Enterprise Linux 7 Installation Guide* .
  - *Red Hat Satellite 6.2 Provisioning Guide*
  - *Red Hat CloudForms 5.0 Provisioning Virtual Machines and Hosts*
  - Automating Configuration Tasks using Ansible in the *Administration Guide*.
- Set the system time zone for all machines in your deployment to UTC. This ensures that data collection and connectivity are not interrupted by variations in your local time zone, such as daylight savings time.
- Use Network Time Protocol (NTP) on all hosts and virtual machines in the environment in order to synchronize time. Authentication and certificates are particularly sensitive to time skew. Using **chronyd** is recommended over **ntpd**. See the following sections of the *Red Hat Enterprise Linux 7 System Administrator's Guide*:
  - Configuring NTP Using the chrony Suite
  - Synchronizing the System Clock with a Remote Server
- Document everything, so that anyone who works with the environment is aware of its current state and required procedures.

4.2. SECURITY RECOMMENDATIONS

- Do not disable any security features (such as HTTPS, SELinux, and the firewall) on the hosts or virtual machines.
- Register all hosts and Red Hat Enterprise Linux virtual machines to either the Red Hat Content Delivery Network or Red Hat Satellite in order to receive the latest security updates and errata.
- Create individual administrator accounts, instead of allowing many people to use the default **admin** account, for proper activity tracking.
- Limit access to the hosts and create separate logins. Do not create a single **root** login for everyone to use. See Managing Users and Groups in the *Red Hat Enterprise Linux 7 System Administrator's Guide*.
- Do not create untrusted users on hosts.
- When deploying the Red Hat Enterprise Linux hosts, only install packages and services required to satisfy virtualization, performance, security, and monitoring requirements. Production hosts should not have additional packages such as analyzers, compilers, or other components that add unnecessary security risk.

4.3. HOST RECOMMENDATIONS

- Standardize the hosts in the same cluster. This includes having consistent hardware models and firmware versions. Mixing different server hardware within the same cluster can result in inconsistent performance from host to host.
- Although you can use both Red Hat Enterprise Linux host and Red Hat Virtualization Host in the same cluster, this configuration should only be used when it serves a specific business or technical requirement.
- Configure fencing devices at deployment time. Fencing devices are required for high availability.
- Use separate hardware switches for fencing traffic. If monitoring and fencing go over the same switch, that switch becomes a single point of failure for high availability.

4.4. NETWORKING RECOMMENDATIONS

- Bond network interfaces, especially on production hosts. Bonding improves the overall availability of service, as well as network bandwidth. See Network Bonding in the *Administration Guide*.
- For optimal performance and simplified troubleshooting, use VLANs to separate different traffic types and make the best use of 10 GbE or 40 GbE networks.
- If the underlying switches support jumbo frames, set the MTU to the maximum size (for example, **9000**) that the underlying switches support. This setting enables optimal throughput, with higher bandwidth and reduced CPU usage, for most applications. The default MTU is determined by the minimum size supported by the underlying switches. If you have LLDP enabled, you can see the MTU supported by the peer of each host in the NIC's tool tip in the **Setup Host Networks** window.

IMPORTANT

If you change the network's **MTU** settings, you must propagate this change to the running virtual machines on the network: Hot unplug and replug every virtual machine's vNIC that should apply the MTU setting, or restart the virtual machines. Otherwise, these interfaces fail when the virtual machine migrates to another host. For more information, see https://access.redhat.com/solutions/4540631 and BZ#1766414.

- 1 GbE networks should only be used for management traffic. Use 10 GbE or 40 GbE for virtual machines and Ethernet-based storage.
- If additional physical interfaces are added to a host for storage use, uncheck **VM network** so that the VLAN is assigned directly to the physical interface.
- If Red Hat OpenStack Platform is deployed, you can integrate Red Hat Virtualization with OpenStack Networking (neutron) to add Open vSwitch capabilities.

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 +ivp4.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 +ivp4.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.

4.5. SELF-HOSTED ENGINE RECOMMENDATIONS

- Create a separate data center and cluster for the Red Hat Virtualization Manager and other infrastructure-level services, if the environment is large enough to allow it. Although the Manager virtual machine can run on hosts in a regular cluster, separation from production virtual machines helps facilitate backup schedules, performance, availability, and security.
- A storage domain dedicated to the Manager virtual machine is created during self-hosted engine deployment. Do not use this storage domain for any other virtual machines.
- If you are anticipating heavy storage workloads, separate the migration, management, and storage networks to reduce the impact on the Manager virtual machine's health.
- Although there is technically no hard limit on the number of hosts per cluster, limit self-hosted engine nodes to 7 nodes per cluster. Distribute the servers in a way that allows better resilience (such as in different racks).
- All self-hosted engine nodes should have an equal CPU family so that the Manager virtual machine can safely migrate between them. If you intend to have various families, begin the installation with the lowest one.

- If the Manager virtual machine shuts down or needs to be migrated, there must be enough memory on a self-hosted engine node for the Manager virtual machine to restart on or migrate to it.