Red Hat Enterprise Linux 9.0 Beta

Configuring and managing virtualization

Setting up your host, creating and administering virtual machines, and understanding virtualization features in Red Hat Enterprise Linux 9
Red Hat Enterprise Linux 9.0 Beta Configuring and managing virtualization

Setting up your host, creating and administering virtual machines, and understanding virtualization features in Red Hat Enterprise Linux 9
Abstract
This document describes how to manage virtualization in Red Hat Enterprise Linux 9 (RHEL 9). In addition to general information about virtualization, it describes how to manage virtualization using command-line utilities, as well as using the web console.
### Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL BETA RELEASE</td>
<td>4</td>
</tr>
<tr>
<td>MAKING OPEN SOURCE MORE INCLUSIVE</td>
<td>5</td>
</tr>
<tr>
<td>PROVIDING FEEDBACK ON RED HAT DOCUMENTATION</td>
<td>6</td>
</tr>
<tr>
<td><strong>CHAPTER 1. INTRODUCING VIRTUALIZATION IN RHEL</strong></td>
<td>7</td>
</tr>
<tr>
<td>1.1. WHAT IS VIRTUALIZATION?</td>
<td>7</td>
</tr>
<tr>
<td>1.2. ADVANTAGES OF VIRTUALIZATION</td>
<td>7</td>
</tr>
<tr>
<td>1.3. VIRTUAL MACHINE COMPONENTS AND THEIR INTERACTION</td>
<td>8</td>
</tr>
<tr>
<td>1.4. TOOLS AND INTERFACES FOR VIRTUALIZATION MANAGEMENT</td>
<td>9</td>
</tr>
<tr>
<td>1.5. RED HAT VIRTUALIZATION SOLUTIONS</td>
<td>10</td>
</tr>
<tr>
<td><strong>CHAPTER 2. ENABLING VIRTUALIZATION</strong></td>
<td>12</td>
</tr>
<tr>
<td><strong>CHAPTER 3. CREATING VIRTUAL MACHINES</strong></td>
<td>14</td>
</tr>
<tr>
<td>3.1. CREATING VIRTUAL MACHINES USING THE COMMAND-LINE INTERFACE</td>
<td>14</td>
</tr>
<tr>
<td>3.2. CREATING VIRTUAL MACHINES AND INSTALLING GUEST OPERATING SYSTEMS USING THE WEB CONSOLE</td>
<td>17</td>
</tr>
<tr>
<td>3.2.1. Creating virtual machines using the web console</td>
<td>17</td>
</tr>
<tr>
<td>3.2.2. Creating virtual machines by importing disk images using the web console</td>
<td>18</td>
</tr>
<tr>
<td>3.2.3. Installing guest operating systems using the web console</td>
<td>18</td>
</tr>
<tr>
<td><strong>CHAPTER 4. STARTING VIRTUAL MACHINES</strong></td>
<td>20</td>
</tr>
<tr>
<td>4.1. STARTING A VIRTUAL MACHINE USING THE COMMAND-LINE INTERFACE</td>
<td>20</td>
</tr>
<tr>
<td>4.2. STARTING VIRTUAL MACHINES USING THE WEB CONSOLE</td>
<td>21</td>
</tr>
<tr>
<td><strong>CHAPTER 5. CONNECTING TO VIRTUAL MACHINES</strong></td>
<td>22</td>
</tr>
<tr>
<td>5.1. INTERACTING WITH VIRTUAL MACHINES USING THE WEB CONSOLE</td>
<td>22</td>
</tr>
<tr>
<td>5.1.1. Viewing the virtual machine graphical console in the web console</td>
<td>22</td>
</tr>
<tr>
<td>5.1.2. Viewing the graphical console in a remote viewer using the web console</td>
<td>23</td>
</tr>
<tr>
<td>5.1.3. Viewing the virtual machine serial console in the web console</td>
<td>24</td>
</tr>
<tr>
<td>5.2. OPENING A VIRTUAL MACHINE GRAPHICAL CONSOLE USING VIRT VIEWER</td>
<td>25</td>
</tr>
<tr>
<td>5.3. CONNECTING TO A VIRTUAL MACHINE USING SSH</td>
<td>26</td>
</tr>
<tr>
<td>5.4. OPENING A VIRTUAL MACHINE SERIAL CONSOLE</td>
<td>27</td>
</tr>
<tr>
<td>5.5. SETTING UP EASY ACCESS TO REMOTE VIRTUALIZATION HOSTS</td>
<td>28</td>
</tr>
<tr>
<td><strong>CHAPTER 6. SHUTTING DOWN VIRTUAL MACHINES</strong></td>
<td>31</td>
</tr>
<tr>
<td>6.1. SHUTTING DOWN A VIRTUAL MACHINE USING THE COMMAND-LINE INTERFACE</td>
<td>31</td>
</tr>
<tr>
<td>6.2. SHUTTING DOWN AND RESTARTING VIRTUAL MACHINES USING THE WEB CONSOLE</td>
<td>31</td>
</tr>
<tr>
<td>6.2.1. Shutting down virtual machines in the web console</td>
<td>31</td>
</tr>
<tr>
<td>6.2.2. Restarting virtual machines using the web console</td>
<td>32</td>
</tr>
<tr>
<td>6.2.3. Sending non-maskable interrupts to VMs using the web console</td>
<td>33</td>
</tr>
<tr>
<td><strong>CHAPTER 7. DELETING VIRTUAL MACHINES</strong></td>
<td>34</td>
</tr>
<tr>
<td>7.1. DELETING VIRTUAL MACHINES USING THE COMMAND LINE INTERFACE</td>
<td>34</td>
</tr>
<tr>
<td>7.2. DELETING VIRTUAL MACHINES USING THE WEB CONSOLE</td>
<td>34</td>
</tr>
<tr>
<td><strong>CHAPTER 8. MANAGING VIRTUAL MACHINES IN THE WEB CONSOLE</strong></td>
<td>36</td>
</tr>
<tr>
<td>8.1. OVERVIEW OF VIRTUAL MACHINE MANAGEMENT USING THE WEB CONSOLE</td>
<td>36</td>
</tr>
<tr>
<td>8.2. SETTING UP THE WEB CONSOLE TO MANAGE VIRTUAL MACHINES</td>
<td>36</td>
</tr>
<tr>
<td><strong>CHAPTER 9. CONFIGURING VIRTUAL MACHINE NETWORK CONNECTIONS</strong></td>
<td>38</td>
</tr>
<tr>
<td>9.1. UNDERSTANDING VIRTUAL NETWORKING</td>
<td>38</td>
</tr>
<tr>
<td>9.1.1. How virtual networks work</td>
<td>38</td>
</tr>
</tbody>
</table>
9.1.2. Virtual networking default configuration
9.2. USING THE WEB CONSOLE FOR MANAGING VIRTUAL MACHINE NETWORK INTERFACES
9.2.1. Viewing and editing virtual network interface information in the web console
9.2.2. Adding and connecting virtual network interfaces in the web console
9.2.3. Disconnecting and removing virtual network interfaces in the web console
9.3. RECOMMENDED VIRTUAL MACHINE NETWORKING CONFIGURATIONS USING THE COMMAND-LINE INTERFACE
9.3.1. Configuring externally visible virtual machines using the command-line interface
9.3.2. Isolating virtual machines from each other using the command-line interface
9.4. RECOMMENDED VIRTUAL MACHINE NETWORKING CONFIGURATIONS USING THE WEB CONSOLE
9.4.1. Configuring externally visible virtual machines using the web console
9.4.2. Isolating virtual machines from each other using the web console
9.5. TYPES OF VIRTUAL MACHINE NETWORK CONNECTIONS
9.5.1. Virtual networking with network address translation
9.5.2. Virtual networking in routed mode
9.5.3. Virtual networking in bridged mode
9.5.4. Virtual networking in isolated mode
9.5.5. Virtual networking in open mode
9.5.6. Direct attachment of the virtual network device
9.5.7. Comparison of virtual machine connection types
9.6. ADDITIONAL RESOURCES

CHAPTER 10. OPTIMIZING VIRTUAL MACHINE PERFORMANCE
10.1. WHAT INFLUENCES VIRTUAL MACHINE PERFORMANCE
The impact of virtualization on system performance
Reducing VM performance loss
10.2. OPTIMIZING VIRTUAL MACHINE PERFORMANCE USING TUNED
10.3. CONFIGURING VIRTUAL MACHINE MEMORY
10.3.1. Adding and removing virtual machine memory using the web console
10.3.2. Adding and removing virtual machine memory using the command-line interface
10.3.3. Additional resources
10.4. OPTIMIZING VIRTUAL MACHINE I/O PERFORMANCE
10.4.1. Tuning block I/O in virtual machines
10.4.2. Disk I/O throttling in virtual machines
10.4.3. Enabling multi-queue virtio-scsi
10.5. OPTIMIZING VIRTUAL MACHINE CPU PERFORMANCE
10.5.1. Adding and removing virtual CPUs using the command-line interface
10.5.2. Managing virtual CPUs using the web console
10.5.3. Configuring NUMA in a virtual machine
10.5.4. Sample vCPU performance tuning scenario
10.5.5. Deactivating kernel same-page merging
10.6. OPTIMIZING VIRTUAL MACHINE NETWORK PERFORMANCE
10.7. VIRTUAL MACHINE PERFORMANCE MONITORING TOOLS
10.8. RELATED INFORMATION
RHEL BETA RELEASE

Red Hat provides Red Hat Enterprise Linux Beta access to all subscribed Red Hat accounts. The purpose of Beta access is to:

- Provide an opportunity to customers to test major features and capabilities prior to the general availability release and provide feedback or report issues.
- Provide Beta product documentation as a preview. Beta product documentation is under development and is subject to substantial change.

Note that Red Hat does not support the usage of RHEL Beta releases in production use cases. For more information, see What does Beta mean in Red Hat Enterprise Linux and can I upgrade a RHEL Beta installation to a General Availability (GA) release?
MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:
  1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.
  2. Use your mouse cursor to highlight the part of text that you want to comment on.
  3. Click the **Add Feedback** pop-up that appears below the highlighted text.
  4. Follow the displayed instructions.

- For submitting more complex feedback, create a Bugzilla ticket:
  1. Go to the [Bugzilla](https://bugzilla.redhat.com) website.
  2. As the Component, use **Documentation**.
  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
  4. Click **Submit Bug**.
CHAPTER 1. INTRODUCING VIRTUALIZATION IN RHEL

If you are unfamiliar with the concept of virtualization or its implementation in Linux, the following sections provide a general overview of virtualization in RHEL 9: its basics, advantages, components, and other possible virtualization solutions provided by Red Hat.

1.1. WHAT IS VIRTUALIZATION?

RHEL 9 provides the virtualization functionality, which enables a machine running RHEL 9 to host multiple virtual machines (VMs), also referred to as guests. VMs use the host’s physical hardware and computing resources to run a separate, virtualized operating system (guest OS) as a user-space process on the host’s operating system.

In other words, virtualization makes it possible to have operating systems within operating systems.

VMs enable you to safely test software configurations and features, run legacy software, or optimize the workload efficiency of your hardware. For more information on the benefits, see Section 1.2, "Advantages of virtualization".

For more information on what virtualization is, see the Red Hat Customer Portal.

Additional resources

- To start using virtualization in Red Hat Enterprise Linux 9, see Chapter 2, Enabling virtualization.
- In addition to Red Hat Enterprise Linux 9 virtualization, Red Hat offers a number of specialized virtualization solutions, each with a different user focus and features. For more information, see Section 1.5, “Red Hat virtualization solutions”.

1.2. ADVANTAGES OF VIRTUALIZATION

Using virtual machines (VMs) has the following benefits in comparison to using physical machines:

- **Flexible and fine-grained allocation of resources**
  A VM runs on a host machine, which is usually physical, and physical hardware can also be assigned for the guest OS to use. However, the allocation of physical resources to the VM is done on the software level, and is therefore very flexible. A VM uses a configurable fraction of the host memory, CPUs, or storage space, and that configuration can specify very fine-grained resource requests.

  For example, what the guest OS sees as its disk can be represented as a file on the host file system, and the size of that disk is less constrained than the available sizes for physical disks.

- **Software-controlled configurations**
  The entire configuration of a VM is saved as data on the host, and is under software control. Therefore, a VM can easily be created, removed, cloned, migrated, operated remotely, or connected to remote storage.

- **Separation from the host**
  A guest OS runs on a virtualized kernel, separate from the host OS. This means that any OS can be installed on a VM, and even if the guest OS becomes unstable or is compromised, the host is not affected in any way.

- **Space and cost efficiency**
  A single physical machine can host a large number of VMs. Therefore, it avoids the need for...
A single physical machine can host a large number of VMs. Therefore, it avoids the need for multiple physical machines to do the same tasks, and thus lowers the space, power, and maintenance requirements associated with physical hardware.

- **Software compatibility**
  Because a VM can use a different OS than its host, virtualization makes it possible to run applications that were not originally released for your host OS. For example, using a RHEL 7 guest OS, you can run applications released for RHEL 7 on a RHEL 9 host system.

\[NOTE\]
Not all operating systems are supported as a guest OS in a RHEL 9 host. For details, see Feature support and limitations in RHEL 9 virtualization.

### 1.3. VIRTUAL MACHINE COMPONENTS AND THEIR INTERACTION

Virtualization in RHEL 9 consists of the following principal software components:

#### Hypervisor

The basis of creating virtual machines (VMs) in RHEL 9 is the **hypervisor**, a software layer that controls hardware and enables running multiple operating systems on a host machine.

The hypervisor includes the **Kernel-based Virtual Machine (KVM)** module and virtualization kernel drivers, such as **virtio** and **vfio**. These components ensure that the Linux kernel on the host machine provides resources for virtualization to user-space software.

At the user-space level, the **QEMU** emulator simulates a complete virtualized hardware platform that the guest operating system can run in, and manages how resources are allocated on the host and presented to the guest.

In addition, the **libvirt** software suite serves as a management and communication layer, making QEMU easier to interact with, enforcing security rules, and providing a number of additional tools for configuring and running VMs.

#### XML configuration

A host-based XML configuration file (also known as a **domain XML** file) determines all settings and devices in a specific VM. The configuration includes:

- Metadata such as the name of the VM, time zone, and other information about the VM.
- A description of the devices in the VM, including virtual CPUs (vCPUs), storage devices, input/output devices, network interface cards, and other hardware, real and virtual.
- VM settings such as the maximum amount of memory it can use, restart settings, and other settings about the behavior of the VM.

For more information on the contents of an XML configuration, see Viewing information about virtual machines.

#### Component interaction

When a VM is started, the hypervisor uses the XML configuration to create an instance of the VM as a user-space process on the host. The hypervisor also makes the VM process accessible to the host-based interfaces, such as the **virsh**, **virt-install**, and **guestfish** utilities, or the web console GUI.
When these virtualization tools are used, libvirt translates their input into instructions for QEMU. QEMU communicates the instructions to KVM, which ensures that the kernel appropriately assigns the resources necessary to carry out the instructions. As a result, QEMU can execute the corresponding user-space changes, such as creating or modifying a VM, or performing an action in the VM’s guest operating system.

**NOTE**

While QEMU is an essential component of the architecture, it is not intended to be used directly on RHEL 9 systems, due to security concerns. Therefore, using `qemu-*` commands is not supported by Red Hat, and it is highly recommended to interact with QEMU using libvirt.

For more information on the host-based interfaces, see Section 1.4, “Tools and interfaces for virtualization management”.

Figure 1.1. RHEL 9 virtualization architecture

1.4. TOOLS AND INTERFACES FOR VIRTUALIZATION MANAGEMENT

You can manage virtualization in RHEL 9 using the command-line interface (CLI) or several graphical user interfaces (GUIs).

**Command-line interface**

The CLI is the most powerful method of managing virtualization in RHEL 9. Prominent CLI commands for virtual machine (VM) management include:

- **virsh** - A versatile virtualization command-line utility and shell with a great variety of purposes, depending on the provided arguments. For example:
  - Starting and shutting down a VM - `virsh start` and `virsh shutdown`
  - Listing available VMs - `virsh list`
  - Creating a VM from a configuration file - `virsh create`
• Entering a virtualization shell - **virsh**

  For more information, see the **virsh(1)** man page.

• **virt-install** - A CLI utility for creating new VMs. For more information, see the **virt-install(1)** man page.

• **virt-xml** - A utility for editing the configuration of a VM.

• **guestfish** - A utility for examining and modifying VM disk images. For more information, see the **guestfish(1)** man page.

**Graphical interfaces**

You can use the following GUIs to manage virtualization in RHEL 9:

• The **RHEL 9 web console**, also known as **Cockpit**, provides a remotely accessible and easy to use graphical user interface for managing VMs and virtualization hosts.

  For instructions on basic virtualization management with the web console, see Chapter 8, *Managing virtual machines in the web console*.

**1.5. RED HAT VIRTUALIZATION SOLUTIONS**

The following Red Hat products are built on top of RHEL 9 virtualization features and expand the KVM virtualization capabilities available in RHEL 9. In addition, many limitations of RHEL 9 virtualization do not apply to these products:

**Red Hat Virtualization (RHV)**

RHV is designed for enterprise-class scalability and performance, and enables the management of your entire virtual infrastructure, including hosts, virtual machines, networks, storage, and users from a centralized graphical interface.

Red Hat Virtualization can be used by enterprises running large deployments or mission-critical applications. Examples of large deployments suited to Red Hat Virtualization include databases, trading platforms, and messaging systems that must run continuously without any downtime.

For more information about Red Hat Virtualization, see the Red Hat Customer Portal or the Red Hat Virtualization documentation suite.

To download a fully supported 60-day evaluation version of Red Hat Virtualization, see the Red Hat Customer Portal.

**Red Hat OpenStack Platform (RHOSP)**

Red Hat OpenStack Platform offers an integrated foundation to create, deploy, and scale a secure and reliable public or private OpenStack cloud.

For more information about Red Hat OpenStack Platform, see the Red Hat Customer Portal or the Red Hat OpenStack Platform documentation suite.

**NOTE**

For details on virtualization features not supported on RHEL but supported on RHV or RHOSP, see Unsupported features in RHEL 9 virtualization.

In addition, specific Red Hat products provide *operating-system-level virtualization*, also known as **containerization**.
• Containers are isolated instances of the host OS and operate on top of an existing OS kernel. For more information on containers, see the Red Hat Customer Portal.

• Containers do not have the versatility of KVM virtualization, but are more lightweight and flexible to handle. For a more detailed comparison, see the Introduction to Linux Containers.
CHAPTER 2. ENABLING VIRTUALIZATION

To use virtualization in RHEL 9, you must install virtualization packages, and ensure your system is configured to host virtual machines (VMs).

Prerequisites

- Red Hat Enterprise Linux 9 is installed and registered on your host machine.
- Your system meets the following hardware requirements to work as a virtualization host:
  - The architecture of your host machine supports KVM virtualization.
  - The following minimum system resources are available:
    - 6 GB free disk space for the host, plus another 6 GB for each intended VM.
    - 2 GB of RAM for the host, plus another 2 GB for each intended VM.

Procedure

1. Install the `virt-install` and `virt-viewer` packages:
   
   ```
   # yum install qemu-kvm libvirt virt-install virt-viewer
   ```

2. Start the `libvirtd` service.
   
   ```
   # systemctl start libvirtd
   ```

Verification

1. Verify that your system is prepared to be a virtualization host:
   
   ```
   # virt-host-validate
   [...]
   QEMU: Checking for device assignment IOMMU support : PASS
   QEMU: Checking if IOMMU is enabled by kernel : WARN (IOMMU appears to be disabled in kernel. Add intel_iommu=on to kernel cmdline arguments)
   LXC: Checking for Linux >= 2.6.26 : PASS
   [...]
   LXC: Checking for cgroup 'blkio' controller mount-point : PASS
   LXC: Checking if device /sys/fs/fuse/connections exists : FAIL (Load the 'fuse' module to enable /proc/ overrides)
   ```

2. If all `virt-host-validate` checks return a **PASS** value, your system is prepared for creating VMs. If any of the checks return a **FAIL** value, follow the displayed instructions to fix the problem.

   If any of the checks return a **WARN** value, consider following the displayed instructions to improve virtualization capabilities.
NOTE

If virtualization is not supported by your host CPU, `virt-host-validate` generates the following output:

QEMU: Checking for hardware virtualization: FAIL (Only emulated CPUs are available, performance will be significantly limited)

However, attempting to create VMs on such a host system will fail, rather than have performance problems.

Next steps

- Create a virtual machine on your RHEL 9 host
CHAPTER 3. CREATING VIRTUAL MACHINES

To create a virtual machine (VM) in RHEL 9, use the command-line interface or the RHEL 9 web console.

3.1. CREATING VIRTUAL MACHINES USING THE COMMAND-LINE INTERFACE

To create a virtual machine (VM) on your RHEL 9 host using the virt-install utility, follow the instructions below.

Prerequisites

- Virtualization is enabled on your host system.
- You have sufficient a amount of system resources to allocate to your VMs, such as disk space, RAM, or CPUs. The recommended values may vary significantly depending on the intended tasks and workload of the VMs.
- An operating system (OS) installation source is available locally or on a network. This can be one of the following:
  - An ISO image of an installation medium
  - A disk image of an existing VM installation

**WARNING**

Installing from a host CD-ROM or DVD-ROM device is not possible in RHEL 9. If you select a CD-ROM or DVD-ROM as the installation source when using any VM installation method available in RHEL 9, the installation will fail. For more information, see the Red Hat Knowledgebase.

Optional: A Kickstart file can be provided for faster and easier configuration of the installation.

Procedure

To create a VM and start its OS installation, use the virt-install command, along with the following mandatory arguments:

- The name of the new machine (\texttt{--name})
- The amount of allocated memory (\texttt{--memory})
- The number of allocated virtual CPUs (\texttt{--vcpus})
- The type and size of the allocated storage (\texttt{--disk})
- The type and location of the OS installation source (\texttt{--cdrom} or \texttt{--location})
Based on the chosen installation method, the necessary options and values can vary. See below for examples:

- The following creates a VM named `demo-guest1` that installs the Windows 10 OS from an ISO image locally stored in the `/home/username/Downloads/Win10install.iso` file. This VM is also allocated with 2048 MiB of RAM and 2 vCPUs, and an 80 GiB qcow2 virtual disk is automatically configured for the VM.

  ```bash
  # virt-install --name demo-guest1 --memory 2048 --vcpus 2 --disk size=80 --os-variant win10 --cdrom /home/username/Downloads/Win10install.iso
  ```

- The following creates a VM named `demo-guest2` that uses the `/home/username/Downloads/rhel9.iso` image to run a RHEL 9 OS from a live CD. No disk space is assigned to this VM, so changes made during the session will not be preserved. In addition, this VM is allocated with 4096 MiB of RAM and 4 vCPUs.

  ```bash
  # virt-install --name demo-guest2 --memory 4096 --vcpus 4 --disk none --livedvd --os-variant rhel9.0 --cdrom /home/username/Downloads/rhel9.iso
  ```

- The following creates a RHEL 9 VM named `demo-guest3` that connects to an existing disk image, `/home/username/backup/disk.qcow2`. This is similar to physically moving a hard drive between machines, so the OS and data available to `demo-guest3` are determined by how the image was handled previously. In addition, this VM is allocated with 2048 MiB of RAM and 2 vCPUs.

  ```bash
  # virt-install --name demo-guest3 --memory 2048 --vcpus 2 --os-variant rhel9.0 --import --disk /home/username/backup/disk.qcow2
  ```

  Note that the `--os-variant` option is highly recommended when importing a disk image. If it is not provided, the performance of the created VM will be negatively affected.

- The following creates a VM named `demo-guest4` that installs from the `http://example.com/OS-install` URL. For the installation to start successfully, the URL must contain a working OS installation tree. In addition, the OS is automatically configured using the `/home/username/ks.cfg` kickstart file. This VM is also allocated with 2048 MiB of RAM, 2 vCPUs, and a 160 GiB qcow2 virtual disk.

  ```bash
  # virt-install --name demo-guest4 --memory 2048 --vcpus 2 --disk size=160 --os-variant rhel9.0 --location http://example.com/OS-install --initrd-inject /home/username/ks.cfg --extra-args="inst.ks=file:/ks.cfg console=tty0 console=ttyS0,115200n8"
  ```

- The following creates a VM named `demo-guest5` that installs from a RHEL9.iso image file in text-only mode, without graphics. It connects the guest console to the serial console. The VM has 16384 MiB of memory, 16 vCPUs, and 280 GiB disk. This kind of installation is useful when connecting to a host over a slow network link.

  ```bash
  # virt-install --name demo-guest5 --memory 16384 --vcpus 16 --disk size=280 --os-variant rhel9.0 --location RHEL9.iso --graphics none --extra-args='console=ttyS0'
  ```

- The following creates a VM named `demo-guest6`, which has the same configuration as `demo-guest5`, but resides on the 10.0.0.1 remote host.
If the VM is created successfully, a virt-viewer window opens with a graphical console of the VM and starts the guest OS installation.

Troubleshooting

- If virt-install fails with a cannot find default network error:
  
  a. Ensure that the libvirt-daemon-config-network package is installed:

  ```
  # yum info libvirt-daemon-config-network
  Installed Packages
  Name : libvirt-daemon-config-network
  [...]
  ```

  b. Verify that the libvirt default network is active and configured to start automatically:

  ```
  # virsh net-list --all
  Name   State   Autostart Persistent
  -------- ----------- ---------------
  default active   yes         yes
  ```

  c. If it is not, activate the default network and set it to auto-start:

  ```
  # virsh net-autostart default
  Network default marked as autostarted

  # virsh net-start default
  Network default started
  ```

  i. If activating the default network fails with the following error, the libvirt-daemon-config-network package has not been installed correctly.

  ```
  error: failed to get network 'default'
  error: Network not found: no network with matching name 'default'
  ```

  To fix this, re-install libvirt-daemon-config-network.

  ```
  # yum reinstall libvirt-daemon-config-network
  ```

  ii. If activating the default network fails with an error similar to the following, a conflict has occurred between the default network’s subnet and an existing interface on the host.

  ```
  error: Failed to start network default
  error: internal error: Network is already in use by interface ens2
  ```

  To fix this, use the virsh net-edit default command and change the 192.168.122.* values in the configuration to a subnet not already in use on the host.

Additional resources
A number of other options can be specified for `virt-install` to further configure the VM and its OS installation. For details, see the `virt-install` man page.

### 3.2. CREATING VIRTUAL MACHINES AND INSTALLING GUEST OPERATING SYSTEMS USING THE WEB CONSOLE

To manage virtual machines (VMs) in a GUI on a RHEL 9 host, use the web console. The following sections provide information on how to use the RHEL 9 web console to create VMs and install guest operating systems on them.

#### 3.2.1. Creating virtual machines using the web console

To create a virtual machine (VM) on the host machine to which the web console is connected, follow the instructions below.

**Prerequisites**

- Virtualization is enabled on your host system.
- The web console VM plug-in is installed on your system.
- You have sufficient a amount of system resources to allocate to your VMs, such as disk space, RAM, or CPUs. The recommended values may vary significantly depending on the intended tasks and workload of the VMs.

**Procedure**

1. In the Virtual Machines interface of the web console, click **Create VM**. The Create new virtual machine dialog appears.

2. Enter the basic configuration of the VM you want to create.
   
   - **Name** - The name of the VM.
   - **Connection** - The type of libvirt connection, system or session. For more details, see TODO: xref to RHEL 9 documentation of system and session connections.
   - **Installation type** - The installation can use a local installation medium, a URL, a PXE network boot, or download an OS from a limited set of operating systems.
   - **Operating system** - The VM’s operating system. Note that Red Hat provides support only for a limited set of guest operating systems.
   - **Storage** - The type of storage with which to configure the VM.
   - **Size** - The amount of storage space with which to configure the VM.
   - **Memory** - The amount of memory with which to configure the VM.
   - **Run unattended installation** - Whether or not to run the installation unattended. This option is available only when the **Installation type** is **Download an OS**.
   - **Immediately Start VM** - Whether or not the VM will start immediately after it is created.

3. Click **Create**.
The VM is created. If the **Immediately Start VM** checkbox is selected, the VM will immediately start and begin installing the guest operating system.

### Additional resources

- For information on installing an operating system on a VM, see Section 3.2.3, "Installing guest operating systems using the web console".

### 3.2.2. Creating virtual machines by importing disk images using the web console

To create a virtual machine (VM) by importing a disk image of an existing VM installation, follow the instructions below.

#### Prerequisites

- The web console VM plug-in is installed on your system.
- You have sufficient amount of system resources to allocate to your VMs, such as disk space, RAM, or CPUs. The recommended values can vary significantly depending on the intended tasks and workload of the VMs.
- Make sure you have a disk image of an existing VM installation

#### Procedure

1. In the **Virtual Machines** interface of the web console, click **Import VM**. The Import a virtual machine dialog appears.

2. Enter the basic configuration of the VM you want to create.
   - **Name** - The name of the VM.
   - **Connection** - The type of libvirt connection, system or session. For more details, see System and session connections.
   - **Disk image** - The path to the existing disk image of a VM on the host system.
   - **Operating system** - The VM’s operating system. Note that Red Hat provides support only for a limited set of guest operating systems.
   - **Memory** - The amount of memory with which to configure the VM.
   - **Immediately start VM** - Whether or not the VM will start immediately after it is created.

3. Click **Import**.

### 3.2.3. Installing guest operating systems using the web console

The first time a virtual machine (VM) loads, you must install an operating system on the VM.

**NOTE**

If the **Immediately Start VM** checkbox in the Create New Virtual Machine dialog is checked, the installation routine of the operating system starts automatically when the VM is created.
Prerequisites

- The web console VM plug-in is installed on your system.
- A VM on which to install an operating system must be available.

Procedure

1. In the Virtual Machines interface, click the VM on which you want to install a guest OS. A new page opens with basic information about the selected VM and controls for managing various aspects of the VM.

2. Optional: Change the firmware.

   **NOTE**
   You can change the firmware only if you had not selected the Immediately Start VM check box in the Create New Virtual Machine dialog, and the OS has not already been installed on the VM.

   a. Click the firmware.
   b. In the Change Firmware window, select the desired firmware.
   c. Click Save.

3. Click Install. The installation routine of the operating system runs in the VM console.

Troubleshooting

- If the installation routine fails, the VM must be deleted and recreated.
CHAPTER 4. STARTING VIRTUAL MACHINES

To start a virtual machine (VM) in RHEL 9, you can use the command line interface or the web console GUI.

Prerequisites

- Before a VM can be started, it must be created and, ideally, also installed with an OS. For instruction to do so, see Chapter 3, Creating virtual machines.

4.1. STARTING A VIRTUAL MACHINE USING THE COMMAND-LINE INTERFACE

You can use the command line interface to start a shut-down virtual machine (VM) or restore a saved VM. Follow the procedure below.

Prerequisites

- An inactive VM that is already defined.
- The name of the VM.
- For remote VMs:
  - The IP address of the host where the VM is located.
  - Root access privileges to the host.

Procedure

- For a local VM, use the `virsh start` utility.
  For example, the following command starts the `demo-guest1` VM.

  # virsh start demo-guest1
  Domain demo-guest1 started

- For a VM located on a remote host, use the `virsh start` utility along with the QEMU+SSH connection to the host.
  For example, the following command starts the `demo-guest1` VM on the 192.168.123.123 host.

  # virsh -c qemu+ssh://root@192.168.123.123/system start demo-guest1

  root@192.168.123.123's password:
  Last login: Mon Feb 18 07:28:55 2019

  Domain demo-guest1 started

Additional Resources

- For more `virsh start` arguments, use `virsh start --help`.
- For simplifying VM management on remote hosts, see modifying your libvirt and SSH configuration.
You can use the `virsh autostart` utility to configure a VM to start automatically when the host boots up. For more information about autostart, see the `virsh autostart` help page.

4.2. STARTING VIRTUAL MACHINES USING THE WEB CONSOLE

If a virtual machine (VM) is in the shut off state, you can start it using the RHEL 9 web console.

**Prerequisites**

- The web console VM plug-in is installed on your system.
- An inactive VM that is already defined.
- The name of the VM.

**Procedure**

1. In the Virtual Machines interface, click the VM you want to start. A new page opens with detailed information about the selected VM and controls for shutting down and deleting the VM.

2. Click Run. The VM starts, and you can connect to its console or graphical output.

3. Optional: To set up the VM to start automatically when the host starts, click the Autostart checkbox.

**Additional resources**

- For information on shutting down a VM, see Section 6.2.1, “Shutting down virtual machines in the web console”.
- For information on restarting a VM, see Section 6.2.2, “Restarting virtual machines using the web console”.
CHAPTER 5. CONNECTING TO VIRTUAL MACHINES

To interact with a virtual machine (VM) in RHEL 9, you need to connect to it by doing one of the following:

- When using the web console interface, use the Virtual Machines pane in the web console interface. For more information, see Section 5.1, “Interacting with virtual machines using the web console”.

- If you need to interact with a VM graphical display without using the web console, use the Virt Viewer application. For details, see Section 5.2, “Opening a virtual machine graphical console using Virt Viewer”.

- When a graphical display is not possible or not necessary, use an SSH terminal connection.

- When the virtual machine is not reachable from your system by using a network, use the virsh console.

If the VMs to which you are connecting are on a remote host rather than a local one, you can optionally configure your system for more convenient access to remote hosts.

Prerequisites

- The VMs you want to interact with are installed and started.

5.1. INTERACTING WITH VIRTUAL MACHINES USING THE WEB CONSOLE

To interact with a virtual machine (VM) in the RHEL 9 web console, you need to connect to the VM’s console. These include both graphical and serial consoles.

- To interact with the VM’s graphical interface in the web console, use the graphical console.

- To interact with the VM’s graphical interface in a remote viewer, use the graphical console in remote viewers.

- To interact with the VM’s CLI in the web console, use the serial console.

5.1.1. Viewing the virtual machine graphical console in the web console

Using the virtual machine (VM) console interface, you can view the graphical output of a selected VM in the RHEL 9 web console.

Prerequisites

- The web console VM plug-in is installed on your system.

- Ensure that both the host and the VM support a graphical interface.

Procedure

1. In the Virtual Machines interface, click the VM whose graphical console you want to view. A new page opens with an Overview and a Console section for the VM.
2. Select **VNC console** in the console drop down menu. The VNC console appears below the menu in the web interface.

   The graphical console appears in the web interface.

3. Click **Expand**

   You can now interact with the VM console using the mouse and keyboard in the same manner you interact with a real machine. The display in the VM console reflects the activities being performed on the VM.

   **NOTE**

   The host on which the web console is running may intercept specific key combinations, such as **Ctrl+Alt+Del**, preventing them from being sent to the VM.

   To send such key combinations, click the **Send key** menu and select the key sequence to send.

   For example, to send the **Ctrl+Alt+Del** combination to the VM, click the **Send key** and select the **Ctrl+Alt+Del** menu entry.

**Additional resources**

- For instructions on viewing the graphical console in a remote viewer, see Section 5.1.2, “Viewing the graphical console in a remote viewer using the web console”.

- For instructions on viewing the serial console in the web console, see Section 5.1.3, “Viewing the virtual machine serial console in the web console”.

### 5.1.2. Viewing the graphical console in a remote viewer using the web console

Using the web console interface, you can display the graphical console of a selected virtual machine (VM) in a remote viewer, such as Virt Viewer.

**NOTE**

You can launch Virt Viewer from within the web console. Other VNC and SPICE remote viewers can be launched manually.

**Prerequisites**

- The web console VM plug-in is installed on your system.

- Ensure that both the host and the VM support a graphical interface.

- Before you can view the graphical console in Virt Viewer, you must install Virt Viewer on the machine to which the web console is connected.

1. Click **Launch remote viewer**.

   A .vv file downloads.

2. Open the file to launch Virt Viewer.
NOTE

Remote Viewer is available on most operating systems. However, some browser extensions and plug-ins do not allow the web console to open Virt Viewer.

Procedure

1. In the Virtual Machines interface, click the VM whose graphical console you want to view. A new page opens with an Overview and a Console section for the VM.

2. Select Desktop Viewer in the console drop down menu.

3. Click Launch Remote Viewer.
   The graphical console opens in Virt Viewer.

   You can interact with the VM console using the mouse and keyboard in the same manner you interact with a real machine. The display in the VM console reflects the activities being performed on the VM.

NOTE

The server on which the web console is running can intercept specific key combinations, such as Ctrl+Alt+Del, preventing them from being sent to the VM.

To send such key combinations, click the Send key menu and select the key sequence to send.

For example, to send the Ctrl+Alt+Del combination to the VM, click the Send key menu and select the Ctrl+Alt+Del menu entry.

Troubleshooting

- If launching the Remote Viewer in the web console does not work or is not optimal, you can manually connect with any viewer application using the following protocols:

  - Address - The default address is 127.0.0.1. You can modify the vnc_listen or the spice_listen parameter in /etc/libvirt/qemu.conf to change it to the host’s IP address.
  - SPICE port - 5900
  - VNC port - 5901

Additional resources

- For instructions on viewing the graphical console in the web console, see Section 5.1.1, “Viewing the virtual machine graphical console in the web console”.

- For instructions on viewing the serial console in the web console, see Section 5.1.3, “Viewing the virtual machine serial console in the web console”.

5.1.3. Viewing the virtual machine serial console in the web console

You can view the serial console of a selected virtual machine (VM) in the RHEL 9 web console. This is useful when the host machine or the VM is not configured with a graphical interface.
For more information about the serial console, see Section 5.4, “Opening a virtual machine serial console”.

Prerequisites

- The web console VM plug-in is installed on your system.

Procedure

1. In the Virtual Machines pane, click the VM whose serial console you want to view. A new page opens with an Overview and a Console section for the VM.
2. Select Serial console in the console drop down menu. The graphical console appears in the web interface.

You can disconnect and reconnect the serial console from the VM.

- To disconnect the serial console from the VM, click Disconnect.
- To reconnect the serial console to the VM, click Reconnect.

Additional resources

- For instructions on viewing the graphical console in the web console, see Section 5.1.1, “Viewing the virtual machine graphical console in the web console”.
- For instructions on viewing the graphical console in a remote viewer, see Section 5.1.2, “Viewing the graphical console in a remote viewer using the web console”.

5.2. OPENING A VIRTUAL MACHINE GRAPHICAL CONSOLE USING VIRT VIEWER

To connect to a graphical console of a KVM virtual machine (VM) and open it in the Virt Viewer desktop application, follow the procedure below.

Prerequisites

- Your system, as well as the VM you are connecting to, must support graphical displays.
- If the target VM is located on a remote host, connection and root access privileges to the host are needed.
- Optional: If the target VM is located on a remote host, set up your libvirt and SSH for more convenient access to remote hosts.

Procedure

- To connect to a local VM, use the following command and replace guest-name with the name of the VM you want to connect to:

  # virt-viewer guest-name
To connect to a remote VM, use the `virt-viewer` command with the SSH protocol. For example, the following command connects as root to a VM called `guest-name`, located on remote system 10.0.0.1. The connection also requires root authentication for 10.0.0.1.

```
# virt-viewer --direct --connect qemu+ssh://root@10.0.0.1/system guest-name
```

If the connection works correctly, the VM display is shown in the **Virt Viewer** window.

You can interact with the VM console using the mouse and keyboard in the same manner you interact with a real machine. The display in the VM console reflects the activities being performed on the VM.

**Additional resources**

- For more information on using Virt Viewer, see the `virt-viewer` man page.
- Connecting to VMs on a remote host can be simplified by modifying your libvirt and SSH configuration.
- For management of VMs in an interactive GUI in RHEL 9, you can use the web console interface. For more information, see Section 5.1, “Interacting with virtual machines using the web console”.

### 5.3. CONNECTING TO A VIRTUAL MACHINE USING SSH

To interact with the terminal of a virtual machine (VM) using the SSH connection protocol, follow the procedure below:

**Prerequisites**

- You have network connection and root access privileges to the target VM.
- If the target VM is located on a remote host, you also have connection and root access privileges to that host.
- The `libvirt-nss` component is installed and enabled on the VM’s host. If it is not, do the following:
  
  a. Install the `libvirt-nss` package:

  ```
  # yum install libvirt-nss
  ```
  
  b. Edit the `/etc/nsswitch.conf` file and add `libvirt_guest` to the `hosts` line:

  ```
  [...]  
  passwd: compat  
  shadow: compat  
  group: compat  
  hosts: files libvirt_guest dns  
  [...]  
  ```

**Procedure**

1. Optional: When connecting to a remote VM, SSH into its physical host first. The following
1. **Optional**: When connecting to a remote VM, SSH into its physical host first. The following example demonstrates connecting to a host machine 10.0.0.1 using its root credentials:

```
# ssh root@10.0.0.1
root@10.0.0.1's password:
Last login: Mon Sep 24 12:05:36 2018
root~#
```

2. Use the VM’s name and user access credentials to connect to it. For example, the following connects to to the “testguest1” VM using its root credentials:

```
# ssh root@testguest1
root@testguest1's password:
Last login: Wed Sep 12 12:05:36 2018
root~#
```

**Troubleshooting**

- If you do not know the VM’s name, you can list all VMs available on the host using the `virsh list` -all command:

```
# virsh list --all

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>testguest1</td>
<td>running</td>
</tr>
<tr>
<td>-</td>
<td>testguest2</td>
<td>shut off</td>
</tr>
</tbody>
</table>
```

5.4. OPENING A VIRTUAL MACHINE SERIAL CONSOLE

Using the `virsh console` command, it is possible to connect to the serial console of a virtual machine (VM).

This is useful when the VM:

- Does not provide VNC or SPICE protocols, and thus does not offer video display for GUI tools.
- Does not have a network connection, and thus cannot be interacted with using SSH.

**Prerequisites**

- The VM must have the serial console configured in its kernel command line. To verify this, the `cat /proc/cmdline` command output on the VM should include `console=ttyS0`. For example:

```
# cat /proc/cmdline

BOOT_IMAGE=/vmlinuz-3.10.0-948.el7.x86_64 root=/dev/mapper/rhel-root ro console=ttys0 console=ttyS0,9600n8 rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb
```

If the serial console is not set up properly on a VM, using `virsh console` to connect to the VM connects you to an unresponsive guest console. However, you can still exit the unresponsive console by using the `Ctrl+]` shortcut.

- To set up serial console on the VM, do the following:
a. On the VM, edit the `/etc/default/grub` file and add `console=ttyS0` to the line that starts with `GRUB_CMDLINE_LINUX`.

b. Clear the kernel options that may prevent your changes from taking effect.

```bash
# grub2-editenv -unset kernelopts
```

c. Reload the Grub configuration:

```bash
# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-948.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-948.el7.x86_64.img
[...]
done
```

d. Reboot the VM.

Procedure

1. On your host system, use the `virsh console` command. The following example connects to the `guest1` VM, if the libvirt driver supports safe console handling:

   ```bash
   # virsh console guest1 --safe
   Connected to domain guest1
   Escape character is ^]
   Subscription-name
   Kernel 3.10.0-948.el7.x86_64 on an x86_64
   localhost login:
   ```

   2. You can interact with the virsh console in the same way as with a standard command-line interface.

Additional resources

- For more information about the VM serial console, see the virsh man page.

5.5. SETTING UP EASY ACCESS TO REMOTE VIRTUALIZATION HOSTS

When managing VMs on a remote host system using libvirt utilities, it is recommended to use the `-c qemu+ssh://root@hostname/system` syntax. For example, to use the `virsh list` command as root on the 10.0.0.1 host:

```bash
# virsh -c qemu+ssh://root@10.0.0.1/system list
root@10.0.0.1's password:
Last login: Mon Feb 18 07:28:55 2019

   Id Name       State
    ---- ----       ------
      1 remote-guest running
```
However, for convenience, you can remove the need to specify the connection details in full by modifying your SSH and libvirt configuration. For example, you will be able to do:

```
# virsh -c remote-host list
```

```
root@10.0.0.1’s password:
Last login: Mon Feb 18 07:28:55 2019
```

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>remote-guest</td>
<td>running</td>
</tr>
</tbody>
</table>

To enable this improvement, follow the instructions below.

**Procedure**

1. Edit or create the `~/.ssh/config` file and add the following to it, where `host-alias` is a shortened name associated with a specific remote host, and `hosturl` is the URL address of the host.

   ```
   Host host-alias
   User root
   Hostname hosturl
   ```

   For example, the following sets up the `tyrannosaurus` alias for root@10.0.0.1:

   ```
   Host tyrannosaurus
   User root
   Hostname 10.0.0.1
   ```

2. Edit or create the `/etc/libvirt/libvirt.conf` file, and add the following, where `qemu-host-alias` is a host alias that QEMU and libvirt utilities will associate with the intended host:

   ```
   uri_aliases = [
   "qemu-host-alias=qemu+ssh://host-alias/system",
   ]
   ```

   For example, the following uses the `tyrannosaurus` alias configured in the previous step to set up the `t-rex` alias, which stands for `qemu+ssh://10.0.0.1/system`:

   ```
   uri_aliases = [
   "t-rex=qemu+ssh://tyrannosaurus/system",
   ]
   ```

3. As a result, you can manage remote VMs by using libvirt-based utilities on the local system with an added `-c qemu-host-alias` parameter. This automatically performs the commands over SSH on the remote host.

   For example, the following lists VMs on the 10.0.0.1 remote host, the connection to which was set up as `t-rex` in the previous steps:

   ```
   $ virsh -c t-rex list
   ```
4. Optional: If you want to use libvirt utilities exclusively on a single remote host, you can also set a specific connection as the default target for libvirt-based utilities. To do so, edit the `/etc/libvirt/libvirt.conf` file and set the value of the `uri_default` parameter to `qemu-host-alias`. For example, the following uses the `t-rex` host alias set up in the previous steps as a default libvirt target.

```bash
# These can be used in cases when no URI is supplied by the application
# (@uri_default also prevents probing of the hypervisor driver).
#
# uri_default = "t-rex"
```

As a result, all libvirt-based commands will automatically be performed on the specified remote host.

```
$ virsh list
root@10.0.0.1’s password:
Last login: Mon Feb 18 07:28:55 2019

   Id   Name      State
-------------
   1    velociraptor  running
```

However, this is not recommended if you also want to manage VMs on your local host or on different remote hosts.

**Additional resources**

- When connecting to a remote host, you can avoid having to provide the root password to the remote system. To do so, use one or more of the following methods:
  - Set up key-based SSH access to the remote host.
  - Use SSH connection multiplexing to connect to the remote system.
  - Set up a kerberos authentication ticket on the remote system. For instructions, see [Kerberos authentication in Identity Management](#).

- Utilities that can use the `-c` (or `--connect`) option and the remote host access configuration described above include:
  - `virt-install`
  - `virt-viewer`
  - `virsh`
  - `virt-manager`
CHAPTER 6. SHUTTING DOWN VIRTUAL MACHINES

To shut down a running virtual machine hosted on RHEL 9, use the command line interface or the web console GUI.

6.1. SHUTTING DOWN A VIRTUAL MACHINE USING THE COMMAND-LINE INTERFACE

To shut down a responsive virtual machine (VM), do one of the following:

- Use a shutdown command appropriate to the guest OS while connected to the guest.

- Use the `virsh shutdown` command on the host:
  
  If the VM is on a local host:
  
  ```
  # virsh shutdown demo-guest1
  Domain demo-guest1 is being shutdown
  ```

  If the VM is on a remote host, in this example 10.0.0.1:
  
  ```
  # virsh -c qemu+ssh://root@10.0.0.1/system shutdown demo-guest1
  root@10.0.0.1's password:
  Last login: Mon Feb 18 07:28:55 2019
  Domain demo-guest1 is being shutdown
  ```

To force a VM to shut down, for example if it has become unresponsive, use the `virsh destroy` command on the host:

```
# virsh destroy demo-guest1
Domain demo-guest1 destroyed
```

NOTE

The `virsh destroy` command does not actually delete or remove the VM configuration or disk images. It only destroys the running VM instance. However, in rare cases, this command may cause corruption of the VM’s file system, so using `virsh destroy` is only recommended if all other shutdown methods have failed.

6.2. SHUTTING DOWN AND RESTARTING VIRTUAL MACHINES USING THE WEB CONSOLE

Using the RHEL 9 web console, you can shut down or restart running virtual machines. You can also send a non-maskable interrupt to an unresponsive virtual machine.

6.2.1. Shutting down virtual machines in the web console

If a virtual machine (VM) is in the running state, you can shut it down using the RHEL 9 web console.

Prerequisites
The web console VM plug-in is installed on your system.

Procedure

1. In the Virtual Machines interface, click the row of the VM you want to shut down. The row expands to reveal the Overview pane with basic information about the selected VM and controls for shutting down and deleting the VM.

2. Click Shut Down. The VM shuts down.

Troubleshooting

- If the VM does not shut down, click the Menu button ⋮ next to the Shut Down button and select Force Shut Down.

- To shut down an unresponsive VM, you can also send a non-maskable interrupt. For more information, see Section 6.2.3, “Sending non-maskable interrupts to VMs using the web console”.

Additional resources

- For information on starting a VM, see Section 4.2, “Starting virtual machines using the web console”.

- For information on restarting a VM, see Section 6.2.2, “Restarting virtual machines using the web console”.

6.2.2. Restarting virtual machines using the web console

If a virtual machine (VM) is in the running state, you can restart it using the RHEL 9 web console.

Prerequisites

- The web console VM plug-in is installed on your system.

Procedure

1. In the Virtual Machines interface, click the row of the VM you want to restart. The row expands to reveal the Overview pane with basic information about the selected VM and controls for shutting down and deleting the VM.

2. Click Restart. The VM shuts down and restarts.

Troubleshooting

- If the VM does not restart, click the Menu button ⋮ next to the Restart button and select Force Restart.

- To restart an unresponsive VM, you can also send a non-maskable interrupt. For more information, see Section 6.2.3, “Sending non-maskable interrupts to VMs using the web console”.
6.2.3. Sending non-maskable interrupts to VMs using the web console

Sending a non-maskable interrupt (NMI) may cause an unresponsive running virtual machine (VM) to respond or shut down. For example, you can send the Ctrl+Alt+Del NMI to a VM that is not responding to standard input.

Prerequisites

- The web console VM plug-in is installed on your system.

Procedure

1. In the Virtual Machines interface, click the row of the VM to which you want to send an NMI. The row expands to reveal the Overview pane with basic information about the selected VM and controls for shutting down and deleting the VM.

2. Click the Menu button ⋮ next to the Shut Down button and select Send Non-Maskable Interrupt. An NMI is sent to the VM.

Additional resources

- For information on starting a VM, see Section 4.2, “Starting virtual machines using the web console”.

- For information on restarting a VM, see Section 6.2.2, “Restarting virtual machines using the web console”.

- For information on shutting down a VM, see Section 6.2.1, “Shutting down virtual machines in the web console”.

CHAPTER 7. DELETING VIRTUAL MACHINES

To delete virtual machines in RHEL 9, use the command line interface or the web console GUI.

7.1. DELETING VIRTUAL MACHINES USING THE COMMAND LINE INTERFACE

To delete a virtual machine (VM), you can remove its XML configuration and associated storage files from the host using the command line. Follow the procedure below:

Prerequisites

- Back up important data from the VM.
- Shut down the VM.
- Make sure no other VMs use the same associated storage.

Procedure

- Use the `virsh undefine` utility.
  For example, the following command removes the `guest1` VM, its associated storage volumes, and non-volatile RAM, if any.

```bash
# virsh undefine guest1 --remove-all-storage --nvram
Domain guest1 has been undefined
Volume 'vda' (/home/images/guest1.qcow2) removed.
```

Additional resources

- For other `virsh undefine` arguments, use `virsh undefine --help` or see the `virsh` man page.

7.2. DELETING VIRTUAL MACHINES USING THE WEB CONSOLE

To delete a virtual machine (VM) and its associated storage files from the host to which the RHEL 9 web console is connected with, follow the procedure below:

Prerequisites

- The web console VM plug-in is installed on your system.
- Back up important data from the VM.
- Make sure no other VM uses the same associated storage.
- Optional: Shut down the VM.

Procedure

1. In the Virtual Machines interface, click the Menu button ⋮ of the VM that you want to delete. A drop down menu appears with controls for various VM operations.

2. Click Delete.
A confirmation dialog appears.

3. **Optional:** To delete all or some of the storage files associated with the VM, select the checkboxes next to the storage files you want to delete.

4. Click **Delete**.
   The VM and any selected storage files are deleted.
CHAPTER 8. MANAGING VIRTUAL MACHINES IN THE WEB CONSOLE

To manage virtual machines in a graphical interface on a RHEL 9 host, you can use the Virtual Machines pane in the RHEL 9 web console.

8.1. OVERVIEW OF VIRTUAL MACHINE MANAGEMENT USING THE WEB CONSOLE

The RHEL 9 web console is a web-based interface for system administration. As one of its features, the web console provides a graphical view of virtual machines (VMs) on the host system, and makes it possible to create, access, and configure these VMs.

Note that to use the web console to manage your VMs on RHEL 9, you must first install a web console plug-in for virtualization.

Next steps

- For instructions on enabling VMs management in your web console, see Setting up the web console to manage virtual machines.

8.2. SETTING UP THE WEB CONSOLE TO MANAGE VIRTUAL MACHINES

Before using the RHEL 9 web console to manage virtual machines (VMs), you must install the web console virtual machine plug-in on the host.

Prerequisites

- Ensure that the web console is installed and enabled on your machine.

```bash
# systemctl status cockpit.socket
cockpit.socket - Cockpit Web Service Socket
Loaded: loaded (/usr/lib/systemd/system/cockpit.socket
[...]
```

If this command returns Unit cockpit.socket could not be found, follow the Installing the web console document to enable the web console.

Procedure

- Install the cockpit-machines plug-in.

```bash
# yum install cockpit-machines
```

Verification

1. Access the web console, for example by entering the https://localhost:9090 address in your browser.

2. Log in.
3. If the installation was successful, **Virtual Machines** appears in the web console side menu.

**Additional resources**

- For instructions on connecting to the web console, as well as other information on using the web console, see the *Managing systems using the RHEL 9 web console* document.
CHAPTER 9. CONFIGURING VIRTUAL MACHINE NETWORK CONNECTIONS

For your virtual machines (VMs) to connect over a network to your host, to other VMs on your host, and to locations on an external network, the VM networking must be configured accordingly. To provide VM networking, the RHEL 9 hypervisor and newly created VMs have a default network configuration, which can also be modified further. For example:

- You can enable the VMs on your host to be discovered and connected to by locations outside the host, as if the VMs were on the same network as the host.
- You can partially or completely isolate a VM from inbound network traffic to increase its security and minimize the risk of any problems with the VM impacting the host.

The following sections explain the various types of VM network configuration and provide instructions for setting up selected VM network configurations.

9.1. UNDERSTANDING VIRTUAL NETWORKING

The connection of virtual machines (VMs) to other devices and locations on a network has to be facilitated by the host hardware. The following sections explain the mechanisms of VM network connections and describe the default VM network setting.

9.1.1. How virtual networks work

Virtual networking uses the concept of a virtual network switch. A virtual network switch is a software construct that operates on a host machine. VMs connect to the network through the virtual network switch. Based on the configuration of the virtual switch, a VM can use an existing virtual network managed by the hypervisor, or a different network connection method.

The following figure shows a virtual network switch connecting two VMs to the network:

From the perspective of a guest operating system, a virtual network connection is the same as a physical network connection. Host machines view virtual network switches as network interfaces. When the `libvirtd` service is first installed and started, it creates `virbr0`, the default network interface for VMs.

To view information about this interface, use the `ip` utility on the host.
By default, all VMs on a single host are connected to the same **NAT-type** virtual network, named **default**, which uses the **virbr0** interface. For details, see Section 9.1.2, “Virtual networking default configuration”.

For basic outbound-only network access from VMs, no additional network setup is usually needed, because the default network is installed along with the **libvirt** package, and is automatically started when the **libvirtd** service is started.

If a different VM network functionality is needed, you can create additional virtual networks and network interfaces and configure your VMs to use them. In addition to the default NAT, these networks and interfaces can be configured to use one of the following modes:

- Routed mode
- Bridged mode
- Isolated mode
- Open mode

### 9.1.2. Virtual networking default configuration

When the **libvirtd** service is first installed on a virtualization host, it contains an initial virtual network configuration in network address translation (NAT) mode. By default, all VMs on the host are connected to the same **libvirt** virtual network, named **default**. VMs on this network can connect to locations both on the host and on the network beyond the host, but with the following limitations:

- VMs on the network are visible to the host and other VMs on the host, but the network traffic is affected by the firewalls in the guest operating system’s network stack and by the **libvirt** network filtering rules attached to the guest interface.

- VMs on the network can connect to locations outside the host but are not visible to them. Outbound traffic is affected by the NAT rules, as well as the host system’s firewall.

The following diagram illustrates the default VM network configuration:
9.2. USING THE WEB CONSOLE FOR MANAGING VIRTUAL MACHINE NETWORK INTERFACES

Using the RHEL 9 web console, you can manage the virtual network interfaces for the virtual machines to which the web console is connected. You can:

- View information about network interfaces and edit them.
- Add network interfaces to virtual machines, and disconnect or delete the interfaces.

9.2.1. Viewing and editing virtual network interface information in the web console

Using the RHEL 9 web console, you can view and modify the virtual network interfaces on a selected virtual machine (VM):

Prerequisites

- The web console VM plug-in is installed on your system.

Procedure

1. In the Virtual Machines interface, click the VM whose information you want to see.
   A new page opens with an Overview section with basic information about the selected VM and a Console section to access the VM’s graphical interface.

2. Scroll to Network Interfaces.
   The Networks Interfaces section displays information about the virtual network interface configured for the VM as well as options to Add, Delete, Edit, or Unplug network interfaces.

   - The information includes the following:
     - Type - The type of network interface for the VM. The types include virtual network, bridge to LAN, and direct attachment.
NOTE

Generic Ethernet connection is not supported in RHEL 9 and later.

- **Model type** - The model of the virtual network interface.
- **MAC Address** - The MAC address of the virtual network interface.
- **IP Address** - The IP address of the virtual network interface.
- **Source** - The source of the network interface. This is dependent on the network type.
- **State** - The state of the virtual network interface.

3. To edit the virtual network interface settings, Click **Edit**. The Virtual Network Interface Settings dialog opens.

4. Change the interface type, source, model, or MAC address.

5. Click **Save**. The network interface is modified.

NOTE

Changes to the virtual network interface settings take effect only after restarting the VM.

Additionally, MAC address can only be modified when the VM is shut off.

### 9.2.2. Adding and connecting virtual network interfaces in the web console

Using the RHEL 9 web console, you can create a virtual network interface and connect a virtual machine (VM) to it.

**Prerequisites**

- The web console VM plug-in is installed on your system.

**Procedure**

1. In the **Virtual Machines** interface, click the VM whose information you want to see.
   A new page opens with an Overview section with basic information about the selected VM and a Console section to access the VM’s graphical interface.

2. Scroll to **Network Interfaces**.
   The Networks Interfaces section displays information about the virtual network interface configured for the VM as well as options to **Add**, **Delete**, **Edit**, or **Plug** network interfaces.

3. Click **Plug** in the row of the virtual network interface you want to connect.
   The selected virtual network interface connects to the VM.

### 9.2.3. Disconnecting and removing virtual network interfaces in the web console

Using the RHEL 9 web console, you can disconnect the virtual network interfaces connected to a selected virtual machine (VM).
Prerequisites

- The web console VM plug-in is installed on your system.

Procedure

1. In the Virtual Machines interface, click the VM whose information you want to see. A new page opens with an Overview section with basic information about the selected VM and a Console section to access the VM's graphical interface.

2. Scroll to Network Interfaces. The Networks Interfaces section displays information about the virtual network interface configured for the VM as well as options to Add, Delete, Edit, or Unplug network interfaces.

3. Click Unplug in the row of the virtual network interface you want to disconnect. The selected virtual network interface disconnects from the VM.

9.3. RECOMMENDED VIRTUAL MACHINE NETWORKING CONFIGURATIONS USING THE COMMAND-LINE INTERFACE

In many scenarios, the default VM networking configuration is sufficient. However, if adjusting the configuration is required, you can use the command-line interface (CLI) to do so. The following sections describe selected VM network setups for such situations.

9.3.1. Configuring externally visible virtual machines using the command-line interface

By default, a newly created VM connects to a NAT-type network that uses virbr0, the default virtual bridge on the host. This ensures that the VM can use the host’s network interface controller (NIC) for connecting to outside networks, but the VM is not reachable from external systems.

If you require a VM to appear on the same external network as the hypervisor, you must use bridged mode instead. To do so, attach the VM to a bridge device connected to the hypervisor’s physical network device. To use the command-line interface for this, follow the instructions below.

Prerequisites

- A shut-down existing VM with the default NAT setup.

- The IP configuration of the hypervisor. This varies depending on the network connection of the host. As an example, this procedure uses a scenario where the host is connected to the network using an ethernet cable, and the hosts' physical NIC MAC address is assigned to a static IP on a DHCP server. Therefore, the ethernet interface is treated as the hypervisor IP.

To obtain the IP configuration of the ethernet interface, use the `ip addr` utility:

```
# ip addr
[...
enp0s25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    group default qlen 1000
    link/ether 54:ee:75:49:dc:46 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.148/24 brd 10.0.0.255 scope global dynamic noprefixroute enp0s25
```

Procedure
1. Create and set up a bridge connection for the physical interface on the host. For instructions, see the Configuring a network bridge. Note that in a scenario where static IP assignment is used, you must move the IPv4 setting of the physical ethernet interface to the bridge interface.

2. Modify the VM’s network to use the created bridged interface. For example, the following sets testguest to use bridge0.

   ```bash
   # virt-xml testguest --edit --network bridge=bridge0
   Domain 'testguest' defined successfully.
   ```

3. Start the VM.

   ```bash
   # virsh start testguest
   ```

4. In the guest operating system, adjust the IP and DHCP settings of the system’s network interface as if the VM was another physical system in the same network as the hypervisor. The specific steps for this will differ depending on the guest OS used by the VM. For example, if the guest OS is RHEL 8, see Configuring an Ethernet connection.

Verification

1. Ensure the newly created bridge is running and contains both the host’s physical interface and the interface of the VM.

   ```bash
   # ip link show master bridge0
   2: enp0s25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bridge0 state UP mode DEFAULT group default qlen 1000
      link/ether 54:ee:75:49:dc:46 brd ff:ff:ff:ff:ff:ff
   10: vnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bridge0 state UNKNOWN mode DEFAULT group default qlen 1000
      link/ether fe:54:00:89:15:40 brd ff:ff:ff:ff:ff:ff
   ```

2. Ensure the VM appears on the same external network as the hypervisor:

   a. In the guest operating system, obtain the network ID of the system. For example, if it is a Linux guest:

      ```bash
      # ip addr
      [...] enp0s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
      link/ether 52:54:00:09:15:46 brd ff:ff:ff:ff:ff:ff
      inet 10.0.0.150/24 brd 10.0.0.255 scope global dynamic noprefixroute enp0s0
      ```

   b. From an external system connected to the local network, connect to the VM using the obtained ID.

      ```bash
      # ssh root@10.0.0.150
      root@10.0.0.150's password:
      Last login: Mon Sep 24 12:05:36 2019
      root~* 
      ```

      If the connection works, the network has been configured successfully.
9.3.2. Isolating virtual machines from each other using the command-line interface

To prevent a virtual machine (VM) from communicating with other VMs on your host, for example to avoid data sharing or to increase system security, you can completely isolate the VM from host-side network traffic.

By default, a newly created VM connects to a NAT-type network that uses `virbr0`, the default virtual bridge on the host. This ensures that the VM can use the host’s NIC for connecting to outside networks, as well as to other VMs on the host. This is a generally secure connection, but in some cases, connectivity to the other VMs may be a security or data privacy hazard. In such situations, you can isolate the VM by using direct `macvtap` connection in private mode instead of the default network.

In private mode, the VM is visible to external systems and can receive a public IP on the host’s subnet, but the VM and the host cannot access each other, and the VM is also not visible to other VMs on the host.

For instructions to set up `macvtap` private mode on your VM using the CLI, see below.

**Prerequisites**

- An existing VM with the default NAT setup.
- The name of the host interface that you want to use for the `macvtap` connection. The interface you must select will vary depending on your use case and the network configuration on your host. As an example, this procedure uses the host’s physical ethernet interface.

To obtain the name of the targeted interface:

```
$ ip addr
[...]
2: enp0s31f6: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
   link/ether 54:e1:ad:42:70:45 brd ff:ff:ff:ff:ff:ff
[...]
```

**Procedure**

- Use the selected interface to set up private `macvtap` on the selected VM. The following example configures `macvtap` in private mode on the `enp0s31f6` interface for the VM named `panic-room`. 
# virt-xml panic-room --edit --network
type=direct,source=enp0s31f6,source.mode=private
Domain panic-room XML defined successfully

Verification

1. Start the updated VM.
   
   # virsh start panic-room
   Domain panic-room started

2. List the interface statistics for the VM.
   
   # virsh domstats panic-room --interface
   Domain: 'panic-room'
   net.count=1
   net.0.name=macvtap0
   net.0.rx.bytes=0
   net.0.rx.pkts=0
   net.0.rx.errs=0
   net.0.rx.drop=0
   net.0.tx.bytes=0
   net.0.tx.pkts=0
   net.0.tx.errs=0
   net.0.tx.drop=0

   If the command displays similar output, the VM has been isolated successfully.

Additional resources

- For instructions on isolating a VM using the web console, see Section 9.4.2, “Isolating virtual machines from each other using the web console”.
- For additional information about macvtap private mode, see Section 9.5.6, “Direct attachment of the virtual network device”.
- For additional security measures that you can set on a VM, see Securing virtual machines in RHEL 9.

9.4. RECOMMENDED VIRTUAL MACHINE NETWORKING CONFIGURATIONS USING THE WEB CONSOLE

In many scenarios, the default VM networking configuration is sufficient. However, if adjusting the configuration is required, you can use the RHEL 9 web console to do so. The following sections describe selected VM network setups for such situations.

9.4.1. Configuring externally visible virtual machines using the web console

By default, a newly created VM connects to a NAT-type network that uses virbr0, the default virtual bridge on the host. This ensures that the VM can use the host’s network interface controller (NIC) for connecting to outside networks, but the VM is not reachable from external systems.
If you require a VM to appear on the same external network as the hypervisor, you must use **bridged mode** instead. To do so, attach the VM to a bridge device connected to the hypervisor’s physical network device. To use the RHEL 9 web console for this, follow the instructions below.

**Prerequisites**

- The web console VM plug-in is installed on your system.
- A shut-down existing VM with the default NAT setup.
- The IP configuration of the hypervisor. This varies depending on the network connection of the host. As an example, this procedure uses a scenario where the host is connected to the network using an ethernet cable, and the hosts’ physical NIC MAC address is assigned to a static IP on a DHCP server. Therefore, the ethernet interface is treated as the hypervisor IP. To obtain the IP configuration of the ethernet interface, go to the **Networking** tab in the web console, and see the **Interfaces** section.

**Procedure**

1. Create and set up a bridge connection for the physical interface on the host. For instructions, see [Configuring network bridges in the web console](#). Note that in a scenario where static IP assignment is used, you must move the IPv4 setting of the physical ethernet interface to the bridge interface.

2. Modify the VM’s network to use the bridged interface. In the **Network Interfaces** tab of the VM:
   
   a. Click **Add Network Interface**
   
   b. In the **Add Virtual Network Interface** dialog, set:
      
      - **Interface Type** to **Bridge to LAN**
      - Source to the newly created bridge, for example `bridge0`
   
   c. Click **Add**
   
   d. **Optional**: Click **Unplug** for all the other interfaces connected to the VM.

3. Click **Run** to start the VM.

4. In the guest operating system, adjust the IP and DHCP settings of the system’s network interface as if the VM was another physical system in the same network as the hypervisor. The specific steps for this will differ depending on the guest OS used by the VM. For example, if the guest OS is RHEL 8, see [Configuring an Ethernet connection](#).

**Verification**

1. In the **Networking** tab of the host’s web console, click the row with the newly created bridge to ensure it is running and contains both the host’s physical interface and the interface of the VM.

2. Ensure the VM appears on the same external network as the hypervisor.
   
   a. In the guest operating system, obtain the network ID of the system. For example, if it is a Linux guest:
   
      ```
      # ip addr
      ```
b. From an external system connected to the local network, connect to the VM using the obtained ID.

```
# ssh root@10.0.0.150
root@110.34.5.18’s password:
Last login: Mon Sep 24 12:05:36 2019
root~#
```

If the connection works, the network has been configured successfully.

**Additional resources**

- For instructions on creating an externally visible VM using the CLI, see Section 9.3.1, “Configuring externally visible virtual machines using the command-line interface”.

- For additional information on bridged mode, see Section 9.5.3, “Virtual networking in bridged mode”.

- In certain situations, such as when using client-to-site VPN while the VM is hosted on the client, using bridged mode for making your VMs available to external locations is not possible. To work around this problem, you can set a destination NAT for the VM. For details, see the Configuring and managing networking document.

**9.4.2. Isolating virtual machines from each other using the web console**

To prevent a virtual machine (VM) from communicating with other VMs on your host, for example to avoid data sharing or to increase system security, you can completely isolate the VM from host-side network traffic.

By default, a newly created VM connects to a NAT-type network that uses `virbr0`, the default virtual bridge on the host. This ensures that the VM can use the host’s NIC for connecting to outside networks, as well as to other VMs on the host. This is a generally secure connection, but in some cases, connectivity to the other VMs may be a security or data privacy hazard. In such situations, you can isolate the VM by using direct `macvtap` connection in private mode instead of the default network.

In private mode, the VM is visible to external systems and can receive a public IP on the host’s subnet, but the VM and the host cannot access each other, and the VM is also not visible to other VMs on the host.

For instructions to set up `macvtap` private mode on your VM using the web console, see below.

**Prerequisites**

- The web console VM plug-in is installed on your system.

- An existing VM with the default NAT setup.

**Procedure**
1. In the Virtual Machines pane, click the row with the virtual machine you want to isolate. A pane with the basic information about the VM opens.

2. Click the Network Interfaces tab.

3. Click Edit. The Virtual Machine Interface Settings dialog opens.

4. Set Interface Type to Direct Attachment.

5. Set Source to the host interface of your choice. Note that the interface you select will vary depending on your use case and the network configuration on your host.

Verification

1. Start the VM by clicking Run.

2. In the Terminal pane of the web console, list the interface statistics for the VM. For example, to view the network interface traffic for the panic-room VM:

   ```
   # virsh domstats panic-room --interface
   Domain: 'panic-room'
   net.count=1
   net.0.name=macvtap0
   net.0.rx.bytes=0
   net.0.rx.pkts=0
   net.0.rx.errs=0
   net.0.rx.drop=0
   net.0.tx.bytes=0
   net.0.tx.pkts=0
   net.0.tx.errs=0
   net.0.tx.drop=0
   ``

   If the command displays similar output, the VM has been isolated successfully.

Additional resources

- For instructions on isolating a VM using the command-line, see Section 9.3.2, “Isolating virtual machines from each other using the command-line interface”.
- For additional information about macvtap private mode, see Section 9.5.6, “Direct attachment of the virtual network device”.
- For additional security measures that you can set on a VM, see Securing virtual machines in RHEL 9.

9.5. TYPES OF VIRTUAL MACHINE NETWORK CONNECTIONS

To modify the networking properties and behavior of your VMs, change the type of virtual network or interface the VMs use. The following sections describe the connection types available to VMs in RHEL 9.

9.5.1. Virtual networking with network address translation

By default, virtual network switches operate in network address translation (NAT) mode. They use IP
masquerading rather than Source-NAT (SNAT) or Destination-NAT (DNAT). IP masquerading enables connected VMs to use the host machine’s IP address for communication with any external network. When the virtual network switch is operating in NAT mode, computers external to the host cannot communicate with the VMs inside the host.

**WARNING**

Virtual network switches use NAT configured by firewall rules. Editing these rules while the switch is running is not recommended, because incorrect rules may result in the switch being unable to communicate.

### 9.5.2. Virtual networking in routed mode

When using *Routed* mode, the virtual switch connects to the physical LAN connected to the host machine, passing traffic back and forth without the use of NAT. The virtual switch can examine all traffic and use the information contained within the network packets to make routing decisions. When using this mode, the virtual machines (VMs) are all in a single subnet, separate from the host machine. The VM subnet is routed through a virtual switch, which exists on the host machine. This enables incoming connections, but requires extra routing-table entries for systems on the external network.

Routed mode uses routing based on the IP address:
Common topologies that use routed mode include DMZs and virtual server hosting.

**DMZ**

You can create a network where one or more nodes are placed in a controlled sub-network for security reasons. Such a sub-network is known as a demilitarized zone (DMZ).

Host machines in a DMZ typically provide services to WAN (external) host machines as well as LAN (internal) host machines. Since this requires them to be accessible from multiple locations, and considering that these locations are controlled and operated in different ways based on their security and trust level, routed mode is the best configuration for this environment.

**Virtual server hosting**

A virtual server hosting provider may have several host machines, each with two physical network connections. One interface is used for management and accounting, the other for the VMs to connect through. Each VM has its own public IP address, but the host machines use private IP addresses so that only internal administrators can manage the VMs.
9.5.3. Virtual networking in bridged mode

In most VM networking modes, VMs automatically create and connect to the `virbr0` virtual bridge. In contrast, in bridged mode, the VM connects to an existing Linux bridge on the host. As a result, the VM is directly visible on the physical network. This enables incoming connections, but does not require any extra routing-table entries.

Bridged mode uses connection switching based on the MAC address:

In bridged mode, the VM appear within the same subnet as the host machine. All other physical machines on the same physical network can detect the VM and access it.

**Bridged network bonding**

It is possible to use multiple physical bridge interfaces on the hypervisor by joining them together with a bond. The bond can then be added to a bridge, after which the VMs can be added to the bridge as well. However, the bonding driver has several modes of operation, and not all of these modes work with a bridge where VMs are in use.

The following **bonding modes** are usable:

- mode 1
- mode 2
- mode 4

In contrast, using modes 0, 3, 5, or 6 is likely to cause the connection to fail. Also note that media-independent interface (MII) monitoring should be used to monitor bonding modes, as Address Resolution Protocol (ARP) monitoring does not work correctly.

For more information on bonding modes, refer to the Red Hat Knowledgebase.

**Common scenarios**

The most common use cases for bridged mode include:

- Deploying VMs in an existing network alongside host machines, making the difference between virtual and physical machines invisible to the end user.
- Deploying VMs without making any changes to existing physical network configuration settings.
- Deploying VMs that must be easily accessible to an existing physical network. Placing VMs on a physical network where they must access DHCP services.
- Connecting VMs to an existing network where virtual LANs (VLANs) are used.

**Additional resources**

- For instructions on configuring your VMs to use bridged mode, see Section 9.3.1, “Configuring externally visible virtual machines using the command-line interface” or Section 9.4.1, “Configuring externally visible virtual machines using the web console”.
- For a detailed explanation of bridge_opts parameters, used to configure bridged networking mode, see the Red Hat Virtualization Administration Guide.

**9.5.4. Virtual networking in isolated mode**

When using isolated mode, virtual machines connected to the virtual switch can communicate with each other and with the host machine, but their traffic will not pass outside of the host machine, and they cannot receive traffic from outside the host machine. Using dnsmasq in this mode is required for basic functionality such as DHCP.
9.5.5. Virtual networking in open mode

When using open mode for networking, libvirt does not generate any firewall rules for the network. As a result, libvirt does not overwrite firewall rules provided by the host, and the user can therefore manually manage the VM’s firewall rules.

9.5.6. Direct attachment of the virtual network device

You can use the macvtap driver to attach a virtual machine’s NIC directly to a specified physical interface of the host machine. The macvtap connection has a number of modes, including private mode.

In this mode, all packets are sent to the external switch and will only be delivered to a target VM on the same host machine if they are sent through an external router or gateway and these send them back to the host. Private mode can be used to prevent the individual VMs on a single host from communicating with each other.

![Diagram of VM to VM and VM to External connections using macvtap](image)

Additional resources

- For instructions on configuring your VMs to use macvtap in private mode, see Section 9.3.2, “Isolating virtual machines from each other using the command-line interface” or Section 9.4.2, “Isolating virtual machines from each other using the web console”.

9.5.7. Comparison of virtual machine connection types

The following table provides information about the locations to which selected types of virtual machine (VM) network configurations can connect, and to which they are visible.

<table>
<thead>
<tr>
<th>Connection to the host</th>
<th>Connection to other VMs on the host</th>
<th>Connection to outside locations</th>
<th>Visible to outside locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridged mode</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>NAT</td>
<td>YES</td>
<td>YES</td>
<td>no</td>
</tr>
<tr>
<td>Routed mode</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Mode</td>
<td>Connection to the host</td>
<td>Connection to other VMs on the host</td>
<td>Connection to outside locations</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------</td>
<td>-------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Isolated mode</td>
<td>YES</td>
<td>YES</td>
<td>no</td>
</tr>
<tr>
<td>Private mode</td>
<td>no</td>
<td>no</td>
<td>YES</td>
</tr>
<tr>
<td>Open mode</td>
<td></td>
<td></td>
<td>Depends on the host’s firewall rules</td>
</tr>
</tbody>
</table>

9.6. ADDITIONAL RESOURCES

- For additional information on networking configurations in RHEL 9, see the Configuring and managing networking document.
- Specific network interface cards can be attached to VMs as SR-IOV devices, which increases their performance. For details, see Managing SR-IOV devices
CHAPTER 10. OPTIMIZING VIRTUAL MACHINE PERFORMANCE

Virtual machines (VMs) always experience some degree of performance deterioration in comparison to the host. The following sections explain the reasons for this deterioration and provide instructions on how to minimize the performance impact of virtualization in RHEL 9, so that your hardware infrastructure resources can be used as efficiently as possible.

10.1. WHAT INFLUENCES VIRTUAL MACHINE PERFORMANCE

VMs are run as user-space processes on the host. The hypervisor therefore needs to convert the host’s system resources so that the VMs can use them. As a consequence, a portion of the resources is consumed by the conversion, and the VM therefore cannot achieve the same performance efficiency as the host.

The impact of virtualization on system performance

More specific reasons for VM performance loss include:

- Virtual CPUs (vCPUs) are implemented as threads on the host, handled by the Linux scheduler.
- VMs do not automatically inherit optimization features, such as NUMA or huge pages, from the host kernel.
- Disk and network I/O settings of the host might have a significant performance impact on the VM.
- Network traffic typically travels to a VM through a software-based bridge.
- Depending on the host devices and their models, there might be significant overhead due to emulation of particular hardware.

The severity of the virtualization impact on the VM performance is influenced by a variety factors, which include:

- The number of concurrently running VMs.
- The amount of virtual devices used by each VM.
- The device types used by the VMs.

Reducing VM performance loss

RHEL 9 provides a number of features you can use to reduce the negative performance effects of virtualization. Notably:

- The tuned service can automatically optimize the resource distribution and performance of your VMs.
- Block I/O tuning can improve the performances of the VM’s block devices, such as disks.
- NUMA tuning can increase vCPU performance.
- Virtual networking can be optimized in various ways.
Tuning VM performance can have adverse effects on other virtualization functions. For example, it can make migrating the modified VM more difficult.

10.2. OPTIMIZING VIRTUAL MACHINE PERFORMANCE USING TUNED

The tuned utility is a tuning profile delivery mechanism that adapts RHEL for certain workload characteristics, such as requirements for CPU-intensive tasks or storage-network throughput responsiveness. It provides a number of tuning profiles that are pre-configured to enhance performance and reduce power consumption in a number of specific use cases. You can edit these profiles or create new profiles to create performance solutions tailored to your environment, including virtualized environments.

Red Hat recommends using the following profiles when using virtualization in RHEL 9:

- For RHEL 9 virtual machines, use the virtual-guest profile. It is based on the generally applicable throughput-performance profile, but also decreases the swappiness of virtual memory.

- For RHEL 9 virtualization hosts, use the virtual-host profile. This enables more aggressive writeback of dirty memory pages, which benefits the host performance.

**Prerequisites**

- The tuned service is installed and enabled.

**Procedure**

To enable a specific tuned profile:

1. List the available tuned profiles.

   ```bash
   # tuned-adm list
   
   Available profiles:
   - balanced - General non-specialized tuned profile
   - desktop  - Optimize for the desktop use-case
   [...]
   - virtual-guest - Optimize for running inside a virtual guest
   - virtual-host  - Optimize for running KVM guests
   Current active profile: balanced
   ```

2. Optional: Create a new tuned profile or edit an existing tuned profile. For more information, see Customizing tuned profiles.

3. Activate a tuned profile.

   ```bash
   # tuned-adm profile selected-profile
   
   To optimize a virtualization host, use the virtual-host profile.
   ```

   ```bash
   # tuned-adm profile virtual-host
   
   On a RHEL guest operating system, use the virtual-guest profile.


Additional resources

- For more information about `tuned` and `tuned` profiles, see Monitoring and managing system status and performance.

## 10.3. CONFIGURING VIRTUAL MACHINE MEMORY

To improve the performance of a virtual machine (VM), you can assign additional host RAM to the VM. Similarly, you can decrease the amount of memory allocated to a VM so the host memory can be allocated to other VMs or tasks.

To perform these actions, you can use the web console or the command-line interface.

### 10.3.1. Adding and removing virtual machine memory using the web console

To improve the performance of a virtual machine (VM) or to free up the host resources it is using, you can use the web console to adjust amount of memory allocated to the VM.

### Prerequisites

- The guest OS is running the memory balloon drivers. To verify this is the case:

  1. Ensure the VM’s configuration includes the `memballoon` device:

    ```bash
    # virsh dumpxml testguest | grep memballoon
    <memballoon model='virtio'>
    </memballoon>
    ```

    If this commands displays any output and the model is not set to `none`, the `memballoon` device is present.

  2. Ensure the balloon drivers are running in the guest OS.

    - In Windows guests, the drivers are installed as a part of the `virtio-win` driver package. For instructions, see Installing paravirtualized KVM drivers for Windows virtual machines.
    
    - In Linux guests, the drivers are generally included by default and activate when the `memballoon` device is present.

- The web console VM plug-in is installed on your system.

### Procedure

1. **Optional:** Obtain the information about the maximum memory and currently used memory for a VM. This will serve as a baseline for your changes, and also for verification.

   ```bash
   # virsh dominfo testguest
   Max memory:    2097152 KiB
   Used memory:   2097152 KiB
   ```

2. In the Virtual Machines interface, click the VM whose information you want to see.
A new page opens with an Overview section with basic information about the selected VM and a
Console section to access the VM’s graphical interface.

3. Click edit next to the Memory line in the Overview pane.
The Memory Adjustment dialog appears.

4. Configure the virtual CPUs for the selected VM.
   - Maximum allocation – Sets the maximum amount of host memory that the VM can use for
     its processes. You can specify the maximum memory when creating the VM or increase it
     later. You can specify memory as multiples of MiB or GiB.
     Adjusting maximum memory allocation is only possible on a shut-off VM.
   
   - Current allocation – Sets the actual amount of memory allocated to the VM. This value can
     be less than the Maximum allocation but cannot exceed it. You can adjust the value to
     regulate the memory available to the VM for its processes. You can specify memory as
     multiples of MiB or GiB.
     If you do not specify this value, the default allocation is the Maximum allocation value.

5. Click Save.
The memory allocation of the VM is adjusted.

Additional resources

- For instructions for adjusting VM memory setting using the command-line interface, see
  Section 10.3.2, "Adding and removing virtual machine memory using the command-line
  interface”.

- To optimize how the VM uses the allocated memory, you can modify your vCPU setting. For
  more information, see Section 10.5, “Optimizing virtual machine CPU performance”.

10.3.2. Adding and removing virtual machine memory using the command-line
    interface

To improve the performance of a virtual machine (VM) or to free up the host resources it is using, you
can use the CLI to adjust amount of memory allocated to the VM.

Prerequisites

- The guest OS is running the memory balloon drivers. To verify this is the case:

  1. Ensure the VM’s configuration includes the memballoon device:

     ```
     # virsh dumpxml testguest | grep memballoon
     <memballoon model="virtio">
     </memballoon>
     ```
     
     If this commands displays any output and the model is not set to none, the memballoon
     device is present.

  2. Ensure the ballon drivers are running in the guest OS.

     - In Windows guests, the drivers are installed as a part of the virtio-win driver package.
       For instructions, see Installing paravirtualized KVM drivers for Windows virtual machines.
In Linux guests, the drivers are generally included by default and activate when the `memballoon` device is present.

**Procedure**

1. **Optional:** Obtain the information about the maximum memory and currently used memory for a VM. This will serve as a baseline for your changes, and also for verification.

   ```bash
   # virsh dominfo testguest
   Max memory: 2097152 KiB
   Used memory: 2097152 KiB
   ```

2. Adjust the maximum memory allocated to a VM. Increasing this value improves the performance potential of the VM, and reducing the value lowers the performance footprint the VM has on your host. Note that this change can only be performed on a shut-off VM, so adjusting a running VM requires a reboot to take effect.

   For example, to change the maximum memory that the testguest VM can use to 4096 MiB:

   ```bash
   # virt-xml testguest --edit --memory memory=4096,currentMemory=4096
   Domain 'testguest' defined successfully.
   Changes will take effect after the domain is fully powered off.
   ```

   1. **Optional:** You can also adjust the memory currently used by the VM, up to the maximum allocation. This regulates the memory load that the VM has on the host until the next reboot, without changing the maximum VM allocation.

   ```bash
   # virsh setmem testguest --current 2048
   ```

**Verification**

1. Confirm that the memory used by the VM has been updated:

   ```bash
   # virsh dominfo testguest
   Max memory: 4194304 KiB
   Used memory: 2097152 KiB
   ```

2. **Optional:** If you adjusted the current VM memory, you can obtain the memory balloon statistics of the VM to evaluate how effectively it regulates its memory use.

   ```bash
   # virsh domstats --balloon testguest
   Domain: 'testguest'
   balloon.current=365624
   balloon.maximum=4194304
   balloon.swap_in=0
   balloon.swap_out=0
   balloon.major_fault=306
   balloon.minor_fault=156117
   balloon.unused=3834448
   balloon.available=4036340
   balloon.usable=3746340
   balloon.last-update=1587971682
   balloon.disk_caches=75444
   ```
Additional resources

- For instructions for adjusting VM memory setting using the web console, see Section 10.3.1, “Adding and removing virtual machine memory using the web console”.

- To optimize how the VM uses the allocated memory, you can modify your vCPU setting. For more information, see Section 10.5, “Optimizing virtual machine CPU performance”.

10.3.3. Additional resources

- To increase the maximum memory of a running VM, you can attach a memory device to the VM. This is also referred to as memory hot plug. For details, see Attaching devices to virtual machines
  Note that removing a memory device from a VM, also known as memory hot unplug, is not supported in RHEL 9, and Red Hat highly discourages its use.

10.4. OPTIMIZING VIRTUAL MACHINE I/O PERFORMANCE

The input and output (I/O) capabilities of a virtual machine (VM) can significantly limit the VM’s overall efficiency. To address this, you can optimize a VM’s I/O by configuring block I/O parameters.

10.4.1. Tuning block I/O in virtual machines

When multiple block devices are being used by one or more VMs, it might be important to adjust the I/O priority of specific virtual devices by modifying their I/O weights.

Increasing the I/O weight of a device increases its priority for I/O bandwidth, and therefore provides it with more host resources. Similarly, reducing a device’s weight makes it consume less host resources.

**NOTE**

Each device’s weight value must be within the 100 to 1000 range. Alternatively, the value can be 0, which removes that device from per-device listings.

Procedure

To display and set a VM’s block I/O parameters:

1. Display the current `<blkio>` parameters for a VM:

```
# virsh dumpxml VM-name
```

```
<domain>
  [...]
  <blkiotune>
    <weight>800</weight>
    <device>
      <path>/dev/sda</path>
      <weight>1000</weight>
    </device>
  </device>
<domain>
```
2. Edit the I/O weight of a specified device:

```
# virsh blkiotune VM-name --device-weights device, I/O-weight
```

For example, the following changes the weight of the /dev/sda device in the liftrul VM to 500.

```
# virsh blkiotune liftrul --device-weights /dev/sda, 500
```

### 10.4.2. Disk I/O throttling in virtual machines

When several VMs are running simultaneously, they can interfere with system performance by using excessive disk I/O. Disk I/O throttling in KVM virtualization provides the ability to set a limit on disk I/O requests sent from the VMs to the host machine. This can prevent a VM from over-utilizing shared resources and impacting the performance of other VMs.

To enable disk I/O throttling, set a limit on disk I/O requests sent from each block device attached to VMs to the host machine.

#### Procedure

1. Use the `virsh domblklist` command to list the names of all the disk devices on a specified VM.

```
# virsh domblklist rollin-coal
Target        Source
----------------------------------
vda           /var/lib/libvirt/images/rollin-coal.qcow2
sda           -
sdb           /home/horridly-demanding-processes.iso
```

2. Find the host block device where the virtual disk that you want to throttle is mounted.

For example, if you want to throttle the sdb virtual disk from the previous step, the following output shows that the disk is mounted on the /dev/nvme0n1p3 partition.

```
$ lsblk
NAME                           MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
zram0                          252:0   0   4G  0 disk  [SWAP]
nvme0n1                        259:0    0 238.5G  0 disk
└─nvme0n1p1                    259:1    0   600M  0 part /boot/efi
└─nvme0n1p2                    259:2    0   1G   0 part /boot
└─nvme0n1p3                    259:3    0 236.9G  0 part
└─luks-a1123911-6f37-463c-b4eb-fxzy1ac12fe 253:0    0 236.9G  0 crypt /home
```

3. Set I/O limits for the block device using the `virsh blkiotune` command.

```
# virsh blkiotune VM-name --parameter device,limit
```
The following example throttles the sdb disk on the rollin-coal VM to 1000 read and write I/O operations per second and to 50 MB per second read and write throughput.

```
# virsh blkio_tune rollin-coal --device-read-iops-sec /dev/nvme0n1p3,1000 --device-write-iops-sec /dev/nvme0n1p3,1000 --device-write-bytes-sec /dev/nvme0n1p3,52428800 --device-read-bytes-sec /dev/nvme0n1p3,52428800
```

Additional information

- Disk I/O throttling can be useful in various situations, for example when VMs belonging to different customers are running on the same host, or when quality of service guarantees are given for different VMs. Disk I/O throttling can also be used to simulate slower disks.

- I/O throttling can be applied independently to each block device attached to a VM and supports limits on throughput and I/O operations.

- Red Hat does not support using the `virsh blkdev_tune` command to configure I/O throttling in VMs. For more information on unsupported features when using RHEL 9 as a VM host, see Unsupported features in RHEL 9 virtualization.

### 10.4.3. Enabling multi-queue virtio-scsi

When using **virtio-scsi** storage devices in your virtual machines (VMs), the **multi-queue virtio-scsi** feature provides improved storage performance and scalability. It enables each virtual CPU (vCPU) to have a separate queue and interrupt to use without affecting other vCPUs.

**Procedure**

- To enable multi-queue virtio-scsi support for a specific VM, add the following to the VM’s XML configuration, where $N$ is the total number of vCPU queues:

  ```xml
  <controller type='scsi' index='0' model='virtio-scsi'>
  <driver queues='N'/>
  </controller>
  ```

**10.5. OPTIMIZING VIRTUAL MACHINE CPU PERFORMANCE**

Much like physical CPUs in host machines, vCPUs are critical to virtual machine (VM) performance. As a result, optimizing vCPUs can have a significant impact on the resource efficiency of your VMs. To optimize your vCPU:

1. Adjust how many host CPUs are assigned to the VM. You can do this using the CLI or the web console.

2. Ensure that the vCPU model is aligned with the CPU model of the host. For example, to set the testguest1 VM to use the CPU model of the host:

   ```
   # virt-xml testguest1 --edit --cpu host-model
   ```

3. Deactivate kernel same-page merging (KSM).

4. If your host machine uses Non-Uniform Memory Access (NUMA), you can also configure NUMA for its VMs. This maps the host’s CPU and memory processes onto the CPU and memory processes of the VM as closely as possible. In effect, NUMA tuning provides the vCPU with a
more streamlined access to the system memory allocated to the VM, which can improve the vCPU processing effectiveness. For details, see Section 10.5.3, “Configuring NUMA in a virtual machine” and Section 10.5.4, “Sample vCPU performance tuning scenario”.

### 10.5.1. Adding and removing virtual CPUs using the command-line interface

To increase or optimize the CPU performance of a virtual machine (VM), you can add or remove virtual CPUs (vCPUs) assigned to the VM.

When performed on a running VM, this is also referred to as vCPU hot plugging and hot unplugging. However, note that vCPU hot unplug is not supported in RHEL 9, and Red Hat highly discourages its use.

### Prerequisites

- **Optional:** View the current state of the vCPUs in the targeted VM. For example, to display the number of vCPUs on the *testguest* VM:

  ```
  # virsh vcpucount testguest
  maximum    config  4
  maximum    live    2
  current    config  2
  current    live    1
  ```

  This output indicates that *testguest* is currently using 1 vCPU, and 1 more vCPU can be hot plugged to it to increase the VM’s performance. However, after reboot, the number of vCPUs *testguest* uses will change to 2, and it will be possible to hot plug 2 more vCPUs.

### Procedure

1. Adjust the maximum number of vCPUs that can be attached to a VM, which takes effect on the VM’s next boot. For example, to increase the maximum vCPU count for the *testguest* VM to 8:

   ```
   # virsh setvcpus testguest 8 --maximum --config
   ```

   Note that the maximum may be limited by the CPU topology, host hardware, the hypervisor, and other factors.

2. Adjust the current number of vCPUs attached to a VM, up to the maximum configured in the previous step. For example:

   - To increase the number of vCPUs attached to the running *testguest* VM to 4:

     ```
     # virsh setvcpus testguest 4 --live
     ```

     This increases the VM’s performance and host load footprint of *testguest* until the VM’s next boot.

   - To permanently decrease the number of vCPUs attached to the *testguest* VM to 1:

     ```
     # virsh setvcpus testguest 1 --config
     ```

   This decreases the VM’s performance and host load footprint of *testguest* after the VM’s next boot.
This decreases the VM’s performance and host load footprint of testguest after the VM’s next boot. However, if needed, additional vCPUs can be hot plugged to the VM to temporarily increase its performance.

**Verification**

- Confirm that the current state of vCPU for the VM reflects your changes.

```bash
# virsh vcpucount testguest
maximum config 8
maximum live 4
current config 1
current live 4
```

**Additional resources**

- For information on adding and removing vCPUs using the web console, see Section 10.5.2, “Managing virtual CPUs using the web console”.

### 10.5.2. Managing virtual CPUs using the web console

Using the RHEL 9 web console, you can review and configure virtual CPUs used by virtual machines (VMs) to which the web console is connected.

**Prerequisites**

- The web console VM plug-in is installed on your system.

**Procedure**

1. In the Virtual Machines interface, click the VM whose information you want to see. A new page opens with an Overview section with basic information about the selected VM and a Console section to access the VM’s graphical interface.

2. Click edit next to the number of vCPUs in the Overview pane. The vCPU details dialog appears.

3. Configure the virtual CPUs for the selected VM.

   - **vCPU Count** - The number of vCPUs currently in use.

     **NOTE**
     
     The vCPU count cannot be greater than the vCPU Maximum.

   - **vCPU Maximum** - The maximum number of virtual CPUs that can be configured for the VM. If this value is higher than the vCPU Count, additional vCPUs can be attached to the VM.

   - **Sockets** - The number of sockets to expose to the VM.

   - **Cores per socket** - The number of cores for each socket to expose to the VM.

   - **Threads per core** - The number of threads for each core to expose to the VM.
Note that the Sockets, Cores per socket and Threads per core options adjust the CPU topology of the VM. This may be beneficial for vCPU performance and may impact the functionality of certain software in the guest OS. If a different setting is not required by your deployment, Red Hat recommends keeping the default values.

4. Click Apply. The virtual CPUs for the VM are configured.

**NOTE**

Changes to virtual CPU settings only take effect after the VM is restarted.

Additional resources:

- For information on managing your vCPUs using the command-line interface, see Section 10.5.1, “Adding and removing virtual CPUs using the command-line interface”.

### 10.5.3. Configuring NUMA in a virtual machine

The following methods can be used to configure Non-Uniform Memory Access (NUMA) settings of a virtual machine (VM) on a RHEL 9 host.

**Prerequisites**

- The host is a NUMA-compatible machine. To detect whether this is the case, use the `virsh nodeinfo` command and see the NUMA cell(s) line:

```bash
# virsh nodeinfo
CPU model:           x86_64
CPU(s):              48
CPU frequency:       1200 MHz
CPU socket(s):       1
Core(s) per socket:  12
Thread(s) per core:  2
NUMA cell(s):        2
Memory size:         67012964 KiB
```

If the value of the line is 2 or greater, the host is NUMA-compatible.

**Procedure**

For ease of use, you can set up a VM’s NUMA configuration using automated utilities and services. However, manual NUMA setup is more likely to yield a significant performance improvement.

**Automatic methods**

- Set the VM’s NUMA policy to **Preferred**. For example, to do so for the `testguest5` VM:

```bash
# virt-xml testguest5 --edit --vcpus placement=auto
# virt-xml testguest5 --edit --numatune mode=preferred
```

- Enable automatic NUMA balancing on the host:

```bash
# echo 1 > /proc/sys/kernel/numa_balancing
```
Use the `numad` command to automatically align the VM CPU with memory resources.

```
# numad
```

### Manual methods

1. Pin specific vCPU threads to a specific host CPU or range of CPUs. This is also possible on non-NUMA hosts and VMs, and is recommended as a safe method of vCPU performance improvement.

   For example, the following commands pin vCPU threads 0 to 5 of the `testguest6` VM to host CPUs 1, 3, 5, 7, 9, and 11, respectively:

```
# virsh vcpupin testguest6 0 1
# virsh vcpupin testguest6 1 3
# virsh vcpupin testguest6 2 5
# virsh vcpupin testguest6 3 7
# virsh vcpupin testguest6 4 9
# virsh vcpupin testguest6 5 11
```

   Afterwards, you can verify whether this was successful:

```
# virsh vcpupin testguest6
VCPU   CPU Affinity
---------------------
0      1
1      3
2      5
3      7
4      9
5      11
```

2. After pinning vCPU threads, you can also pin QEMU process threads associated with a specified VM to a specific host CPU or range of CPUs. For example, the following commands pin the QEMU process thread of `testguest6` to CPUs 13 and 15, and verify this was successful:

```
# virsh emulatorpin testguest6 13,15
# virsh emulatorpin testguest6
emulator: CPU Affinity
-----------------------
*: 13,15
```

3. Finally, you can also specify which host NUMA nodes will be assigned specifically to a certain VM. This can improve the host memory usage by the VM’s vCPU. For example, the following commands set `testguest6` to use host NUMA nodes 3 to 5, and verify this was successful:

```
# virsh numatune testguest6 --nodeset 3-5
# virsh numatune testguest6
```

### Additional resources

- Note that for best performance results, it is recommended to use all of the manual tuning methods listed above. For an example of such a configuration, see Section 10.5.4, “Sample vCPU performance tuning scenario”.

To see the current NUMA configuration of your system, you can use the `numastat` utility. For details on using `numastat`, see Section 10.7, “Virtual machine performance monitoring tools”.

NUMA tuning is currently not possible to perform on IBM Z hosts. For further information, see How virtualization on IBM Z differs from AMD64 and Intel 64.

### 10.5.4. Sample vCPU performance tuning scenario

To obtain the best vCPU performance possible, Red Hat recommends using manual `vcpupin`, `emulatorpin`, and `numatune` settings together, for example like in the following scenario.

#### Starting scenario

- Your host has the following hardware specifics:
  - 2 NUMA nodes
  - 3 CPU cores on each node
  - 2 threads on each core

The output of `virsh nodeinfo` of such a machine would look similar to:

```bash
# virsh nodeinfo
CPU model:           x86_64
CPU(s):              12
CPU frequency:       3661 MHz
CPU socket(s):       2
Core(s) per socket:  3
Thread(s) per core:  2
NUMA cell(s):        2
Memory size:         31248692 KiB
```

You intend to modify an existing VM to have 8 vCPUs, which means that it will not fit in a single NUMA node. Therefore, you should distribute 4 vCPUs on each NUMA node and make the vCPU topology resemble the host topology as closely as possible. This means that vCPUs that run as sibling threads of a given physical CPU should be pinned to host threads on the same core. For details, see the Solution below:

#### Solution

1. Obtain the information on the host topology:

```bash
# virsh capabilities
<topology>
  <cells num="2">
    <cell id="0">
      <memory unit="KiB">15624346</memory>
      <pages unit="KiB" size="4">3906086</pages>
    </cell>
    <cell id="1">
      <memory unit="KiB">15624346</memory>
      <pages unit="KiB" size="4">3906086</pages>
    </cell>
  </cells>
</topology>
```

2. **Optional:** Test the performance of the VM using the applicable tools and utilities.

3. Set up and mount 1 GiB huge pages on the host:
   
   a. Add the following line to the host’s kernel command line:

   ```
   default_hugepagesz=1G hugepagesz=1G
   ```

   b. Create the `/etc/systemd/system/hugetlb-gigantic-pages.service` file with the following content:

   ```
   [Unit]
   Description=HugeTLB Gigantic Pages Reservation
   DefaultDependencies=no
   Before=dev-hugepages.mount
   ConditionPathExists=/sys/devices/system/node
   ConditionKernelCommandLine=hugepagesz=1G

   [Service]
   Type=oneshot
   RemainAfterExit=yes
   ExecStart=/etc/systemd/hugetlb-reserve-pages.sh
   ```
c. Create the `/etc/systemd/hugetlb-reserve-pages.sh` file with the following content:

```bash
#!/bin/sh

nodes_path=/sys/devices/system/node/
if [ ! -d $nodes_path ]; then
    echo "ERROR: $nodes_path does not exist"
    exit 1
fi

reserve_pages()
{
    echo $1 > $nodes_path/$2/hugepages/hugepages-1048576kB/nr_hugepages
}

reserve_pages 4 node1
reserve_pages 4 node2
```

This reserves four 1GiB huge pages from `node1` and four 1GiB huge pages from `node2`.

d. Make the script created in the previous step executable:

```
# chmod +x /etc/systemd/hugetlb-reserve-pages.sh
```

e. Enable huge page reservation on boot:

```
# systemctl enable hugetlb-gigantic-pages
```

4. Use the `virsh edit` command to edit the XML configuration of the VM you wish to optimize, in this example `super-VM`:

```
# virsh edit super-vm
```

5. Adjust the XML configuration of the VM in the following way:

a. Set the VM to use 8 static vCPUs. Use the `<vcpu/>` element to do this.

b. Pin each of the vCPU threads to the corresponding host CPU threads that it mirrors in the topology. To do so, use the `<vcpupin/>` elements in the `<cputune>` section. Note that, as shown by the `virsh capabilities` utility above, host CPU threads are not ordered sequentially in their respective cores. In addition, the vCPU threads should be pinned to the highest available set of host cores on the same NUMA node. For a table illustration, see the `Additional Resources` section below.

The XML configuration for steps a. and b. can look similar to:

```
<cpuset>
  <vcpupin vcpu='0' cpuset='1'/>
  <vcpupin vcpu='1' cpuset='4'/>
  <vcpupin vcpu='2' cpuset='2'/>
```
c. Set the VM to use 1 GiB huge pages:

```xml
<memoryBacking>
    <hugepages>
        <page size='1' unit='GiB'/>
    </hugepages>
</memoryBacking>
```

d. Configure the VM's NUMA nodes to use memory from the corresponding NUMA nodes on the host. To do so, use the `<memnode/>` elements in the `<numatune/>` section:

```xml
<numatune>
    <memory mode="preferred" nodeset="1"/>
    <memnode cellid="0" mode="strict" nodeset="0"/>
    <memnode cellid="1" mode="strict" nodeset="1"/>
</numatune>
```

e. Ensure the CPU mode is set to `host-passthrough`, and that the CPU uses cache in `passthrough` mode:

```xml
<cpu mode="host-passthrough">
    <topology sockets="2" cores="2" threads="2"/>
    <cache mode="passthrough"/>
</cpu>
```

6. The resulting XML configuration of the VM should include a section similar to the following:

```xml
<...>
    <memoryBacking>
        <hugepages>
            <page size='1' unit='GiB'/>
        </hugepages>
    </memoryBacking>
    <vcpu placement='static'>8</vcpu>
    <cputune>
        <vcpupin vcpu='0' cpuset='1'/>
        <vcpupin vcpu='1' cpuset='4'/>
        <vcpupin vcpu='2' cpuset='2'/>
        <vcpupin vcpu='3' cpuset='5'/>
        <vcpupin vcpu='4' cpuset='7'/>
        <vcpupin vcpu='5' cpuset='10'/>
        <vcpupin vcpu='6' cpuset='8'/>
        <vcpupin vcpu='7' cpuset='11'/>
        <emulatorpin cpuset='6,9'/>
    </cputune>
    <numatune>
        <memory mode="preferred" nodeset="1"/>
    </numatune>
</...>
```
Optional: Test the performance of the VM using the applicable tools and utilities to evaluate the impact of the VM’s optimization.

Additional resources

- The following tables illustrate the connections between the vCPUs and the host CPUs they should be pinned to:

**Table 10.1. Host topology**

<table>
<thead>
<tr>
<th>CPU threads</th>
<th>0</th>
<th>3</th>
<th>1</th>
<th>4</th>
<th>2</th>
<th>5</th>
<th>6</th>
<th>9</th>
<th>7</th>
<th>10</th>
<th>8</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>0</td>
<td></td>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
<td>3</td>
<td></td>
<td>4</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Sockets</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NUMA nodes</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 10.2. VM topology**

<table>
<thead>
<tr>
<th>vCPU threads</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>0</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Sockets</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NUMA nodes</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Table 10.3. Combined host and VM topology

<table>
<thead>
<tr>
<th>vCPU threads</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host CPU</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>threads</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Cores</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td>Sockets</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>NUMA nodes</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

In this scenario, there are 2 NUMA nodes and 8 vCPUs. Therefore, 4 vCPU threads should be pinned to each node.

In addition, Red Hat recommends leaving at least a single CPU thread available on each node for host system operations.

Because in this example, each NUMA node houses 3 cores, each with 2 host CPU threads, the set for node 0 translates as follows:

```
< vcpupin vcpu='0' cpuset='1'/>
< vcpupin vcpu='1' cpuset='4'/>
< vcpupin vcpu='2' cpuset='2'/>
< vcpupin vcpu='3' cpuset='5'/>
```

10.5.5. Deactivating kernel same-page merging

Although kernel same-page merging (KSM) improves memory density, it increases CPU utilization, and might adversely affect overall performance depending on the workload. In such cases, you can improve the virtual machine (VM) performance by deactivating KSM.

Depending on your requirements, you can either deactivate KSM for a single session or persistently.

**Procedure**

- To deactivate KSM for a single session, use the `systemctl` utility to stop `ksm` and `ksmtuned` services.

  ```bash
  # systemctl stop ksm
  # systemctl stop ksmtuned
  ```

- To deactivate KSM persistently, use the `systemctl` utility to disable `ksm` and `ksmtuned` services.

  ```bash
  # systemctl disable ksm
  Removed /etc/systemd/system/multi-user.target.wants/ksm.service.
  # systemctl disable ksmtuned
  Removed /etc/systemd/system/multi-user.target.wants/ksmtuned.service.
  ```
NOTE

Memory pages shared between VMs before deactivating KSM will remain shared. To stop sharing, delete all the PageKSM pages in the system using the following command:

```
# echo 2 > /sys/kernel/mm/ksm/run
```

After anonymous pages replace the KSM pages, the khugepaged kernel service will rebuild transparent hugepages on the VM’s physical memory.

10.6. OPTIMIZING VIRTUAL MACHINE NETWORK PERFORMANCE

Due to the virtual nature of a VM’s network interface card (NIC), the VM loses a portion of its allocated host network bandwidth, which can reduce the overall workload efficiency of the VM. The following tips can minimize the negative impact of virtualization on the virtual NIC (vNIC) throughput.

Procedure

Use any of the following methods and observe if it has a beneficial effect on your VM network performance:

Enable the vhost_net module

On the host, ensure the vhost_net kernel feature is enabled:

```
# lsmod | grep vhost
vhost_net 32768 1
vhost 53248 1 vhost_net
tap 24576 1 vhost_net
tun 57344 6 vhost_net
```

If the output of this command is blank, enable the vhost_net kernel module:

```
# modprobe vhost_net
```

Set up multi-queue virtio-net

To set up the multi-queue virtio-net feature for a VM, use the virsh edit command to edit to the XML configuration of the VM. In the XML, add the following to the `<devices>` section, and replace N with the number of vCPUs in the VM, up to 16:

```
<interface type='network'>
  <source network='default'/>
  <model type='virtio'/>
  <driver name='vhost' queues='N'/>
</interface>
```

If the VM is running, restart it for the changes to take effect.

Batching network packets

In Linux VM configurations with a long transmission path, batching packets before submitting them to the kernel may improve cache utilization. To set up packet batching, use the following command on the host, and replace tap0 with the name of the network interface that the VMs use:
# ethtool -C tap0 rx-frames 128

SR-IOV

If your host NIC supports SR-IOV, use SR-IOV device assignment for your vNICs. For more information, see Managing SR-IOV devices.

Additional resources

- For additional information on virtual network connection types and tips for usage, see Section 9.1, “Understanding virtual networking”.

### 10.7. VIRTUAL MACHINE PERFORMANCE MONITORING TOOLS

To identify what consumes the most VM resources and which aspect of VM performance needs optimization, performance diagnostic tools, both general and VM-specific, can be used.

#### Default OS performance monitoring tools

For standard performance evaluation, you can use the utilities provided by default by your host and guest operating systems:

- On your RHEL 9 host, as root, use the `top` utility or the `system monitor` application, and look for `qemu` and `virt` in the output. This shows how much host system resources your VMs are consuming.
  
  If the monitoring tool displays that any of the `qemu` or `virt` processes consume a large portion of the host CPU or memory capacity, use the `perf` utility to investigate. For details, see below.

  In addition, if a `vhost_net` thread process, named for example `vhost_net-1234`, is displayed as consuming an excessive amount of host CPU capacity, consider using virtual network optimization features, such as `multi-queue virtio-net`.

- On the guest operating system, use performance utilities and applications available on the system to evaluate which processes consume the most system resources.
  
  - On Linux systems, you can use the `top` utility.
  
  - On Windows systems, you can use the `Task Manager` application.

#### perf kvm

You can use the `perf` utility to collect and analyze virtualization-specific statistics about the performance of your RHEL 9 host. To do so:

1. On the host, install the `perf` package:

   ```bash
   # yum install perf
   ```

2. Use one of the `perf kvm stat` commands to display perf statistics for your virtualization host:

   - For real-time monitoring of your hypervisor, use the `perf kvm stat live` command.

   - To log the perf data of your hypervisor over a period of time, activate the logging using the `perf kvm stat record` command. After the command is canceled or interrupted, the data is saved in the `perf.data.guest` file, which can be analyzed using the `perf kvm stat report` command.
3. Analyze the `perf` output for types of ***VM-EXIT*** events and their distribution. For example, the `PAUSE_INSTRUCTION` events should be infrequent, but in the following output, the high occurrence of this event suggests that the host CPUs are not handling the running vCPUs well. In such a scenario, consider shutting down some of your active VMs, removing vCPUs from these VMs, or **tuning the performance of the vCPUs**.

```
# perf kvm stat report

Analyze events for all VMs, all VCPUs:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Samples</th>
<th>Samples%</th>
<th>Time%</th>
<th>Min Time</th>
<th>Max Time</th>
<th>Avg time</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXTERNAL_INTERRUPT</td>
<td>365634</td>
<td>31.59%</td>
<td>18.04%</td>
<td>0.42us</td>
<td>58780.59us</td>
<td>1.80us</td>
</tr>
<tr>
<td>MSR_WRITE</td>
<td>293428</td>
<td>25.35%</td>
<td>0.13%</td>
<td>0.59us</td>
<td>17873.02us</td>
<td>3.38us</td>
</tr>
<tr>
<td>PREEMPTION_TIMER</td>
<td>276162</td>
<td>23.86%</td>
<td>0.23%</td>
<td>0.51us</td>
<td>21396.03us</td>
<td>3.80us</td>
</tr>
<tr>
<td>PAUSE_INSTRUCTION</td>
<td>189375</td>
<td>16.36%</td>
<td>11.75%</td>
<td>0.72us</td>
<td>29655.25us</td>
<td>256.77us</td>
</tr>
<tr>
<td>HLT</td>
<td>20440</td>
<td>1.77%</td>
<td>69.83%</td>
<td>0.62us</td>
<td>79319.41us</td>
<td>14134.56us</td>
</tr>
<tr>
<td>VMEXIT</td>
<td>12426</td>
<td>1.07%</td>
<td>0.03%</td>
<td>1.02us</td>
<td>5416.25us</td>
<td>8.77us</td>
</tr>
<tr>
<td>EXCEPTION_NMI</td>
<td>27</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.69us</td>
<td>1.34us</td>
<td>0.98us</td>
</tr>
<tr>
<td>EPT_MISCONFIG</td>
<td>5</td>
<td>0.00%</td>
<td>0.00%</td>
<td>5.15us</td>
<td>10.85us</td>
<td>7.88us</td>
</tr>
</tbody>
</table>

Total Samples:1157497, Total events handled time:413728274.66us.
```

Other event types that can signal problems in the output of `perf kvm stat` include:

- **INSN_EMULATION** - suggests suboptimal VM I/O configuration.

For more information on using `perf` to monitor virtualization performance, see the `perf-kvm` man page.

**numastat**

To see the current NUMA configuration of your system, you can use the `numastat` utility, which is provided by installing the `numactl` package.

The following shows a host with 4 running VMs, each obtaining memory from multiple NUMA nodes. This is not optimal for vCPU performance, and warrants adjusting:

```
# numastat -c qemu-kvm

Per-node process memory usage (in MBs)

<table>
<thead>
<tr>
<th>PID</th>
<th>Node 0</th>
<th>Node 1</th>
<th>Node 2</th>
<th>Node 3</th>
<th>Node 4</th>
<th>Node 5</th>
<th>Node 6</th>
<th>Node 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>51722</td>
<td>68</td>
<td>16</td>
<td>357</td>
<td>6936</td>
<td>2</td>
<td>3</td>
<td>147</td>
<td>598</td>
</tr>
<tr>
<td>51747</td>
<td>245</td>
<td>11</td>
<td>5</td>
<td>18</td>
<td>5172</td>
<td>2532</td>
<td>1</td>
<td>92</td>
</tr>
<tr>
<td>53736</td>
<td>62</td>
<td>432</td>
<td>1661</td>
<td>506</td>
<td>4851</td>
<td>136</td>
<td>22</td>
<td>445</td>
</tr>
</tbody>
</table>
```

---

**CHAPTER 10. OPTIMIZING VIRTUAL MACHINE PERFORMANCE**

75
In contrast, the following shows memory being provided to each VM by a single node, which is significantly more efficient.

```bash
# numastat -c qemu-kvm

Per-node process memory usage (in MBs)

<table>
<thead>
<tr>
<th>PID</th>
<th>Node 0</th>
<th>Node 1</th>
<th>Node 2</th>
<th>Node 3</th>
<th>Node 4</th>
<th>Node 5</th>
<th>Node 6</th>
<th>Node 7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>51747 (qemu-kvm)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>8080</td>
</tr>
<tr>
<td>53736 (qemu-kvm)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>8113</td>
</tr>
<tr>
<td>53773 (qemu-kvm)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>8118</td>
</tr>
<tr>
<td>59065 (qemu-kvm)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8051</td>
</tr>
</tbody>
</table>

| Total | 0      | 0      | 0      | 0      | 0      | 0      | 1      | 0      | 8110  |
```

10.8. RELATED INFORMATION

- When using Windows as the guest operating system of your VM, Red Hat recommends applying additional optimization measures. For details, see Optimizing Windows virtual machines.