Table of Contents

About this document ........................................................................................................................................ v
1 Before You Begin ............................................................................................................................................. 1
2 Getting Started with Oracle Linux Virtualization Manager ........................................................................... 3
   Adding a KVM Compute Host to the Manager ................................................................................................. 3
   Adding Storage .................................................................................................................................................. 4
   Attaching an iSCSI Data Domain ..................................................................................................................... 4
   Uploading Images to the Data Domain ............................................................................................................. 5
   Creating a Logical Network ............................................................................................................................ 7
   Creating a Virtual Machine Network .............................................................................................................. 7
   Assigning the Virtual Machine Network to a KVM Compute Host ............................................................... 8
   Creating a New Virtual Machine ..................................................................................................................... 11
   Creating a New Oracle Linux Virtual Machine ............................................................................................. 11
   Creating a New Microsoft Windows Virtual Machine .................................................................................... 16
   Creating a Template ........................................................................................................................................ 23
   Sealing an Oracle Linux Virtual Machine for Use as a Template ................................................................. 23
   Creating an Oracle Linux Template .............................................................................................................. 24
   Creating a Cloud-Init Enabled Template ....................................................................................................... 25
   Creating a Virtual Machine from a Template .................................................................................................. 27
   Creating an Oracle Linux Virtual Machine from a Template ........................................................................ 27
   Backing Up and Restoring the Manager ......................................................................................................... 29
   Backing Up the Manager ............................................................................................................................... 29
   Restoring a Full Backup of the Manager ........................................................................................................ 30
3 Additional Administration Tasks .................................................................................................................... 33
   Global Configuration ....................................................................................................................................... 33
      Administering User Accounts from the Administration Portal .................................................................. 33
      Administering User and Group Accounts from the Command Line ......................................................... 36
   Data Centers .................................................................................................................................................. 44
      Creating a New Data Center .......................................................................................................................... 44
   Clusters ........................................................................................................................................................... 44
      Creating a New Cluster ................................................................................................................................ 44
   Networks ......................................................................................................................................................... 46
      Customizing vNIC Profiles for Virtual Machines ....................................................................................... 46
   Storage ............................................................................................................................................................ 47
      Preparing Local Storage for a KVM Compute Host ..................................................................................... 47
      Configuring a KVM Compute Host to Use Local Storage ......................................................................... 47
      Preparing NFS Storage ................................................................................................................................ 48
      Attaching an NFS Data Domain .................................................................................................................. 49
      Adding an FC Data Domain .......................................................................................................................... 50
   Virtual Machines .......................................................................................................................................... 50
      Live Editing a Virtual Machine ...................................................................................................................... 50
      Creating a Snapshot of a Virtual Machine ...................................................................................................... 52
      Restoring a Virtual Machine from a Snapshot ............................................................................................ 53
      Creating a Virtual Machine from a Snapshot ............................................................................................. 54
      Deleting a Snapshot ...................................................................................................................................... 54
      Migrating Virtual Machines between Hosts ................................................................................................. 55
   Encrypted Communication .............................................................................................................................. 58
      Replacing the Oracle Linux Virtualization Manager Apache SSL Certificate .......................................... 58
   Event Notifications ........................................................................................................................................ 60
      Configuring Event Notification Services on the Engine ............................................................................. 60
      Creating Event Notifications in the Administration Portal ....................................................................... 61
      Canceling Event Notifications in the Administration Portal .................................................................... 62
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Engine to Send SNMP Traps</td>
<td>62</td>
</tr>
<tr>
<td>4 Deployment Optimization</td>
<td>67</td>
</tr>
<tr>
<td>Optimizing Clusters, Hosts and Virtual Machines</td>
<td>67</td>
</tr>
<tr>
<td>Configuring Memory and CPUs</td>
<td>67</td>
</tr>
<tr>
<td>Configuring a Highly Available Host</td>
<td>69</td>
</tr>
<tr>
<td>Configuring a Highly Available Virtual Machine</td>
<td>72</td>
</tr>
<tr>
<td>Hot Plugging Devices on Virtual Machines</td>
<td>73</td>
</tr>
<tr>
<td>Hot Plugging vCPUs</td>
<td>73</td>
</tr>
<tr>
<td>Hot Plugging Virtual Memory</td>
<td>74</td>
</tr>
</tbody>
</table>
About this document

This document is part of the documentation for Oracle Linux Virtualization Manager, which is available at: http://docs.oracle.com/en/virtualization/oracle-linux-virtualization-manager/index.html

The documentation consists of the following items:

**Oracle Linux Virtualization Manager Release Notes**

This document provides a summary of the new features, changes, fixed bugs, and known issues in the Oracle Linux Virtualization Manager. It contains last-minute information, which may not be included in the main body of documentation.

Read this document before you install your environment.

**Oracle Linux Virtualization Manager Architecture and Planning Guide**

This document provides an architectural overview of Oracle Linux Virtualization Manager, prerequisites, and planning information for your environment.

Read this document before you install your environment.

**Oracle Linux Virtualization Manager Installation Guide**

This document provides an overview of the Oracle Linux Virtualization Manager and explains how to install the Oracle Linux Virtualization Manager environment, including important information, such as system requirements, for planning your virtualization environment.

**Oracle Linux Virtualization Manager Getting Started Guide**

This document explains how to get started with the Oracle Linux Virtualization Manager. It provides an example scenario that covers some of the basic procedures for setting up the environment, such as, adding hosts, adding storage, creating virtual machines, and so on.

Chapter 1 Before You Begin

Before you begin the tasks in this guide, you should be familiar with the concepts that are presented in the Oracle Linux Virtualization Manager Architecture and Planning Guide.

To follow along with the tasks in this guide, ensure the following prerequisites are met:

- The procedures in this guide assume that you have installed Oracle Linux Virtualization Manager in your environment. For more information, refer to Installing the Manager in the Oracle Linux Virtualization Manager Installation Guide.

- For tasks that must be completed in the Manager, the procedures in this guide assume that you are logged in to the Administration Portal.

- Oracle Linux Virtualization Manager creates a default data center and cluster during installation. For the purpose of tutorial, the default data center and cluster are used. For the procedures to create new data centers or a new clusters, refer to Chapter 3, Additional Administration Tasks.

- For Adding a KVM Compute Host to the Manager, you must have access to a host that you can add to your virtualization environment.

- For Adding Storage, an Internet Small Computer System Interface (iSCSI) storage device is used for the example scenario in this guide. If you do not have access to an iSCSI device, refer to Storage for the procedures for adding other storage types to your virtualization environment.

- For Uploading Images to the Data Domain, the ovirt-engine certificate must be registered as a valid CA in the browser to connect to the ovirt-imageio-proxy service.

- For Creating a New Virtual Machine:
  
  - The procedures for creating Oracle Linux and Microsoft Windows VMs assume that you have added the ISO images to the data domain on the storage device used in Adding Storage.

  - To use the console, you must install the Remote Viewer application. This application provides users with a graphical console for connecting to virtual machines.

  1. Install the virt-viewer package.

     ```bash
     # yum install virt-viewer
     ```

  2. Restart your browser for the changes to effect in the Oracle Linux Virtualization Manager.
Chapter 2 Getting Started with Oracle Linux Virtualization Manager

Table of Contents

Adding a KVM Compute Host to the Manager ................................................................. 3
Adding Storage .............................................................................................................. 4
  Attaching an iSCSI Data Domain .............................................................................. 4
  Uploading Images to the Data Domain .................................................................... 5
Creating a Logical Network ......................................................................................... 7
  Creating a Virtual Machine Network ..................................................................... 7
  Assigning the Virtual Machine Network to a KVM Compute Host ....................... 8
Creating a New Virtual Machine .................................................................................. 11
  Creating a New Oracle Linux Virtual Machine ...................................................... 11
  Creating a New Microsoft Windows Virtual Machine ........................................... 16
Creating a Template ...................................................................................................... 23
  Sealing an Oracle Linux Virtual Machine for Use as a Template ......................... 23
  Creating an Oracle Linux Template ....................................................................... 24
  Creating a Cloud-Init Enabled Template .................................................................. 25
Creating a Virtual Machine from a Template ............................................................ 27
  Creating an Oracle Linux Virtual Machine from a Template ............................... 27
Backing Up and Restoring the Manager ..................................................................... 29
  Backing Up the Manager ....................................................................................... 29
  Restoring a Full Backup of the Manager ............................................................... 30

To get you started with Oracle Linux Virtualization Manager, the following example scenario walks you through the procedures for adding hosts, adding storage, setting up a network, creating virtual machines, and backing up and restoring the Manager.

Adding a KVM Compute Host to the Manager

To add a KVM host to the Manager:

1. Go to Compute and then click Hosts.

2. On the Hosts pane, click New.

   The New Host dialog box opens with the General tab selected on the sidebar.

3. From the Host Cluster drop-down list, select the data center and host cluster for the new host.

   By default, the Default option is selected in the drop-down list.

   For this step, leave Default selected from the drop-down list because the default data center and cluster are used for the example scenario.

   For the procedures to create new data centers or a new clusters, refer to Chapter 3, Additional Administration Tasks.

4. For the Name field, enter a name for the new host.

5. For the Hostname field, enter the host name for the new host. You must use the DNS host name for the host.
Adding Storage

6. For the **SSH Port** field, the standard SSH port, port 22, is auto-filled.

7. Under **Authentication**, select the authentication method to use.

   Oracle recommends that you select **SSH PublicKey** authentication. If you select this option, copy the key displayed in the **SSH PublicKey** field to the `/root/.ssh/authorized_keys` file on the host.

   Otherwise, enter the root user's password to use password authentication.

8. **(Optional)** Configure other settings for the new host from the other tabs on the **New Host** sidebar.

9. Click **OK** to add the host to the data center.

   The host is added to the list of hosts in the Manager. While the Manager is installing the host agent (VDSM) and other required packages on the host, the status of the host is shown as **Installing**. You can view the progress of the installation in the details pane. When the host is added to the Manager, the host status changes to **Up**.

Adding Storage

For this example scenario, you attach an iSCSI storage to your virtualization environment and then upload an ISO image to the data domain.

If you do not have access to an iSCSI device, refer to **Storage** for the procedures for adding other storage types to your virtualization environment.

Attaching an iSCSI Data Domain

For iSCSI storage, a storage domain is created from a volume group that is composed of pre-existing LUNs.

To attach an iSCSI data domain to your virtualization enviroment:

1. Go to **Storage** and then click **Domains**.

   The **Storage Domains** pane opens.

2. Click **New Domain**.

   The **New Domain** dialog box opens.

3. For the **Name** field, enter a name for the data domain.

4. From the **Data Center** drop-down list, select the Data Center for which to attach the data domain.

   By default, the **Default** option is selected in the drop-down list.

   For this step, leave **Default** selected from the drop-down list because the default data center and cluster are used for the example scenario.

   For the procedures to create new data centers or a new clusters, refer to Chapter 3, **Additional Administration Tasks**.

5. From the **Domain Function** drop-down list, select the domain function. By default, the **Data** option is selected in the drop-down list.

   For this step, leave **Data** as the domain function because you are creating a data domain in this example.
6. From the **Storage Type** drop-down list, select **iSCSI**.

7. For the **Host to Use** drop-down list, select the host for which to attach the data domain.

   For this example scenario, select the host added in Adding a KVM Compute Host to the Manager.

8. When **iSCSI** is selected for the **Storage Type**, the **Discover Targets** dialog box opens and the **New Domain** dialog box automatically displays the known targets with unused LUNs under the **Target Name** column.

   If the **Discover Targets** dialog box is not visible in the **New Domain** dialog box, make sure that you have selected the **Target > LUNS** view on the left-side of the column.

   If the target from which you are adding storage is not listed, complete the following fields in the **Discover Targets** dialog box:

   a. For the **Address** field, enter fully qualified domain name or IP address of the iSCSI host on the storage array.

   b. For the **Port** field, enter the port to connect to on the host when browsing for targets. By default, this field is automatically populated with the default iSCSI Port, **3260**.

   After completing these fields, click **Discover**.

   The **Target Name** column updates to list all the available targets discovered on the storage array.

9. Under the **Target Name** column, select the desired target and select the black right-directional arrow to log in to the target.

   The **Storage Domains** pane refreshes to list only the targets for which you logged in.

10. Click **+** to expand the desired target.

    The target expands to display all the unused LUNS.

11. Click **Add** for each LUN ID that is to connect to the target.

12. **(Optional)** Configure the advanced parameters.

    If you are using ZFS storage, you must uncheck the **Discard after Delete** option.

13. Click **OK**.

    You can click **Tasks** to monitor the various processing steps that are completed to attach the iSCSI data domain to the data center.

    After the iSCSI data domain has been added to your virtualization environment, you can then upload the ISO images that are used for creating virtual machines in Creating a New Virtual Machine.

### Uploading Images to the Data Domain

Before using the Manager to upload images to the data domain, you must perform the following steps to ensure that the prerequisites for uploading images have been met on the Manager and KVM hosts.

### Before You Begin

To ensure that the prerequisites for uploading images to the data domain have been met:

1. On the engine host, verify that the **ovirt-image-proxy** service has been configured and is running.
Uploading Images to the Data Domain

1. When the service is running, the output displays as follows.

```
# systemctl status ovirt-imageio-proxy.service
```

ovirt-imageio-proxy.service - oVirt ImageIO Proxy
Loaded: loaded (/usr/lib/systemd/system/ovirt-imageio-proxy.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2019-03-25 13:12:29 PDT; 2 weeks 0 days ago
Main PID: 28708 (ovirt-imageio-p)
    CGroup: /system.slice/ovirt-imageio-proxy.service
         └─ 28708 /usr/bin/python2 /usr/bin/ovirt-imageio-proxy
...
```

This service is automatically configured and is started when you run the `engine-setup` command during the installation of the Manager.

2. On the engine host, copy the `ovirt-engine` certificate as a trusted certificate to the `/etc/pki/ca-trust/source/anchors/ovirt.ca.pem` file, or use the correct path of the file:

```
# scp /etc/pki/ovirt-engine/ca.pem
root@image-proxy-address:/etc/pki/ca-trust/source/anchors/ovirt.ca.pem
```

You can obtain the address to enter for the `image-proxy-address` variable by entering the `engine-config --get ImageProxyAddress` command.

3. On the KVM host, verify that the `ovirt-image-proxy` service has been configured and is running. For example:

```
# systemctl status ovirt-imageio-daemon
```

ovirt-imageio-daemon.service - oVirt ImageIO Daemon
Loaded: loaded (/usr/lib/systemd/system/ovirt-imageio-daemon.service; disabled; vendor preset: disabled)
Active: active (running) since Wed 2019-03-27 18:38:36 EDT; 3 weeks 4 days ago
Main PID: 366 (ovirt-imageio-d)
    Tasks: 4
    CGroup: /system.slice/ovirt-imageio-daemon.service
           └─ 366 /usr/bin/python /usr/bin/ovirt-imageio-daemon
Mar 27 18:38:36 myserver systemd[1]: Starting oVirt ImageIO Daemon...
Mar 27 18:38:36 myserver systemd[1]: Started oVirt ImageIO Daemon.
```

4. On the KVM host, ensure the `ovirt-image-proxy` is properly linked by creating a directory for the certificate and then creating a symbolic link to the certificate.

```
# mkdir /etc/pki/ovirt-engine/
# ln -s /etc/pki/ca-trust/source/anchors/ovirt.ca.pem /etc/pki/ovirt-engine/ca.pem
```

5. Verify that the certificate authority has been imported into the web browser used to access the Manager by browsing to the following URL and enabling the trust settings: `https://engine_address/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`

6. Verify that you are using a browser that meets the browser requirement to access the Administration Portal.

   For more information, refer to the Oracle Linux Virtualization Manager Installation Guide.

7. Proceed to Uploading an ISO Image to the Data Domain.
Creating a Logical Network

For this example scenario, you create a virtual machine network that you then assign to the KVM host added in Adding a KVM Compute Host to the Manager. This network is used as the virtual machine network for the virtual machines created in Creating a New Virtual Machine.

Creating a Virtual Machine Network

To create a virtual machine network:

1. Go to Network and then click Networks.
2. On the Networks pane, click New.
3. From the Data Center drop-down list, select the Data Center for the network.
   By default, the Default option is selected in the drop-down list.
   For this step, leave Default selected from the drop-down list because the default data center and cluster are used in this example scenario.
   For the procedures to create new data centers or a new clusters, refer to Chapter 3, Additional Administration Tasks.
4. For the Name field, enter a name for the new network.
5. Leave the the VM Network check box selected.
Under the **Network Parameters** section, the **VM Network** check box is selected by default, which is left selected because a virtual machine network is being created in this example.

6. **(Optional)** Configure other settings for the new logical network from the other tabs on the **New Logical Network** sidebar.

   The default settings are used for this example scenario.

7. Click **OK** to create the network.

   The following screenshot shows the **General** tab of the **New Logical Network** dialog box completed for the new logical network that is being created in this example:

   - From the **Data Center** drop-down list, the **Default** option is selected.
   - For the **Name** field, **vm_pub** is entered.
   - Under the **Network Parameters** section, the **VM Network** check box is selected.

   **Figure 2.1 New Logical Network Dialog Box: General Tab**

---

**Assigning the Virtual Machine Network to a KVM Compute Host**

To assign the virtual machine network to a KVM host:

1. Go to **Compute** and then click **Hosts**.

   The **Hosts** pane opens.

2. Under the **Name** column, click the name of the host for which to add the network.
Assigning the Virtual Machine Network to a KVM Compute Host

The following screenshot shows the **Hosts** pane with the name of the host highlighted in a red rectangular box to emphasize where you need to click to set up a network on a host.

**Figure 2.2 Hosts Pane**

![Hosts Pane Screenshot](image)

After clicking the name of the host, the **General** tab opens with details about the host.

3. Click the **Network Interfaces** tab on the horizontal menu.

The **Network Interfaces** tab opens with details about the network interfaces on the available host.

4. Highlight the network interface that you want to use for the network being added by clicking the row for the respective interface.

5. Click **Setup Host Networks**.

The **Setup Host Networks** dialog box opens for the host. The physical interfaces on the host are listed under the **Interfaces** column and any logical networks assigned to the interface are displayed under the **Assigned Logical Networks** column. Unassigned logical networks are displayed under the **Unassigned Logical Networks** column.

As shown in the following screenshot, the logical network created in Creating a Logical Network named `vm_pub` is displayed under the **Unassigned Logical Networks** column. In the next step, you assign this network to the network interface named `eno2`, which currently has no network assigned to it.
6. Select the network you want to add from the **Unassigned Logical Networks** column by left-clicking the network and, while holding down the mouse, drag the network over to the box to the right of the available network interface where you want to add the network.

Alternatively, you can right-click the network and select the available interface from a drop-down list.

For this example, the logical network named **vm_pub** is assigned to the available network interface named **eno2**. As shown in the following screenshot, after dragging the network from **Unassigned Logical Networks** over to this interface, the network named **vm_pub** appears under the **Assigned Logical Networks** column as assigned to the network interface named **eno2**.
Creating a New Virtual Machine

Before creating new virtual machines for use in your virtualization environment, refer to Chapter 1, *Before You Begin* for more information about the prerequisites for this example scenario.

Creating a New Oracle Linux Virtual Machine

For the example scenario, you create a new Oracle Linux virtual machine, install the Oracle Linux guest OS, and install the Linux guest agent for this Oracle Linux virtual machine.

To create a new Oracle Linux virtual machine:

1. Go to **Compute** and then click **Virtual Machines**.

   The **Virtual Machines** pane opens with the list of virtual machines that have been created.

2. Click **New**.

   The **New Virtual Machine** dialog box opens with the **General** tab selected on the sidebar.

7. After editing the network settings, click **OK** to save the settings.

8. Click **OK** to add the network.
3. From the **Cluster** drop-down list, select the data center and host cluster for the new host.

By default, the **Default** option is selected in the drop-down list.

For this step, leave **Default** selected from the drop-down list because the default data center and cluster are used in this example scenario. For the procedures to create new data centers or a new clusters, refer to **Chapter 3, Additional Administration Tasks**.

4. From the **Operating System** drop-down list, select the operating system for the virtual machine.

5. For the **Name** field, enter a name for the new virtual machine.

6. Under **Instance Images**, add storage to the virtual machine by either using an existing virtual disk or creating a new virtual disk.

   - To use an existing virtual disk, click **Attach** and select the virtual disk to use for the virtual machine storage. Then click **OK**.
   
   - To create a new virtual disk, click **Create** and update the fields for the virtual machine storage or accept the default settings. Then click **OK**.

   For the example scenario, all of the default settings are accepted for the new virtual disk that is being created, except the **Size (GiB)** field, which is set to **4**. The following screenshot shows the **New Virtual Disk** dialog box for the Oracle Linux virtual machine being created in this example scenario.

**Figure 2.5 New Virtual Disk Dialog Box**
7. Connect the virtual machine to a network by adding a network interface. To do that, select the vNIC profile created in Creating a Logical Network from the nic1 drop-down list.

For information about customizing vNICs, refer to Customizing vNIC Profiles for Virtual Machines.

The following screenshot shows the General tab open on the New Virtual Machine dialog box for the new Oracle Linux virtual machine being created in this example scenario. In the dialog box, the following key fields are completed:

- From the Cluster drop-down list, the Default option is selected.
- For the Operating System drop-down list, Oracle Linux 7.x x64 is selected.
- For the Name field, ol7-vm1 is entered.
- Under Instance Images, a virtual disk named ol7-vm1_Disk1 is being created, which has been set to a size of 4GB.
- From the nic1 drop-down list, the logical network named vm_pub is selected.

Figure 2.6 New Virtual Machine Dialog Box
8. Click **Show Advanced Options** to display additional configuration options available for the new virtual machine.

9. *(Optional)* Click the **System** tab on the sidebar to adjust the CPU and memory size for the virtual machine from the defaults.

   For this example scenario the default values are used:
   - For **Memory Size** field, the default value of **1024 MB** is used.
   - For the **Maximum memory** field, the default value of **4096 MB** is used.
   - For the **Total Virtual CPUs** field, the default value of **1** is used.

10. Click the **Boot Options** tab on the sidebar to specify the boot sequence for the virtual device and then select the device from the **First Device** drop-down list.

    In the following screenshot, **CD-ROM** is selected from the **First Device** drop-down list. The **Attach CD** check box is also selected with the appropriate ISO file chosen from the drop-down list. For this example scenario, **OracleLinux-R7-U6-Server-x86_64-dvd.iso** is selected.

**Figure 2.7 New Virtual Machines Dialog Box: Boot Options Tab**
Creating a New Oracle Linux Virtual Machine

After you install the Oracle Linux guest OS, change the First Device from CD-ROM to Hard Disk from the drop-down list. For more information, refer to Installing the Oracle Linux Guest OS.

11. Click OK to create the virtual machine.

12. Proceed to Installing the Oracle Linux Guest OS.

Installing the Oracle Linux Guest OS

To install the Oracle Linux guest OS:

1. Go to Compute and then click Virtual Machines.

   The Virtual Machines pane opens with the list of virtual machines that have been created.

2. Select the virtual machine created in Creating a New Oracle Linux Virtual Machine and click Run.

3. Click Console to open a console to the virtual machine.

   If you have not installed the Remote Viewer application, refer to Chapter 1, Before You Begin.

4. Install the Oracle Linux guest OS.

   Refer to the Oracle Linux Installation Guide for Release 7 for more information on how to install Oracle Linux.

5. After you finish installing the Oracle Linux guest OS, return to the Virtual Machines pane, highlight the row for this virtual machine, and click Edit.

   The Edit Virtual Machines dialog box opens.

6. Click the Boot Options tab on the sidebar of the dialog box to specify the boot sequence for the virtual device and then change CD-ROM to Hard Disk from the First Device drop-down list.

7. Click OK to save the changes to the virtual machine configuration.

   The Oracle Linux virtual machine now boots from the virtual disk where the operating system is installed.

8. (Optional) If you use a proxy server for Internet access, configure Yum with the proxy server settings. For more information, see Configuring Use of a Proxy Server at https://docs.oracle.com/en/operating-systems/oracle-linux/7/admin/ol7-proxy-config.html.

9. (Optional) If you are using yum to update the host, make sure the host is using the modular yum repository configuration. For more information, see Getting Started with Oracle Linux Yum Server at http://yum.oracle.com/getting-started.html.

10. Proceed to Installing the Linux Guest Agent.

Installing the Linux Guest Agent

To install the Linux guest agent:

1. Open a console session for the Oracle Linux guest and log in to the terminal.

2. Install the latest ovirt-guest-agent package, which is available from http://yum.oracle.com/repo/OracleLinux/OL7/ovirt42/x86_64.

   For Oracle Linux 7 guests:

For Oracle Linux 6 guests:


For Oracle Linux 5 guests:

# yum install https://yum.oracle.com/repo/OracleLinux/OL7/ovirt42/x86_64/getPackage/ovirt-guest-agent-version.el5.noarch.rpm

where *version* is the ovirt-guest-agent package number.

3. Start the guest agent service for the Oracle Linux guest.

For Oracle Linux 7 guests:

# systemctl start ovirt-guest-agent.service

For Oracle Linux 6 and Oracle Linux 5 guests:

# service ovirt-guest-agent start

4. *(Optional)* Enable an automatic restart of the guest agent service when the VM is rebooted.

For Oracle Linux 7 guests:

# systemctl enable ovirt-guest-agent.service

For Oracle Linux 6 and Oracle Linux 5 guests:

# chkconfig ovirt-guest-agent on

---

**Creating a New Microsoft Windows Virtual Machine**

For the example scenario, you create a new Microsoft Windows virtual machine, install the Microsoft Windows guest OS, and install the Microsoft Windows guest agent and VirtIO drivers for this virtual machine.

**Before You Begin**

Before creating Microsoft Windows virtual machines, ensure the following prerequisites are met.

1. Install the *ovirt-guest-tools-iso* package on the Manager:

   # yum install ovirt-guest-tools-iso

2. Verify the package installation:

   # rpm -ql ovirt-guest-tools-iso
   /usr/share/ovirt-guest-tools-iso
   /usr/share/ovirt-guest-tools-iso/ovirt-tools-setup.iso
   /usr/share/ovirt-guest-tools-iso/ovirt-tools-setup.iso

**Creating a New Microsoft Windows Virtual Machine**

To create a new Microsoft Windows virtual machine:

1. Go to *Compute* and then click *Virtual Machines*.

   The *Virtual Machines* pane opens with the list of virtual machines that have been created.
2. Click **New**.

   The **New Virtual Machine** dialog box opens with the **General** tab selected on the sidebar.

3. From the **Cluster** drop-down list, select the data center and host cluster for the new host.

   By default, the **Default** option is selected in the drop-down list.

   For this step, leave **Default** selected from the drop-down list because the default data center and cluster are used in this example scenario. For the procedures to create new data centers or a new cluster, refer to **Chapter 3, Additional Administration Tasks**.

4. From the **Operating System** drop-down list, select the appropriate Microsoft Windows operating system for the virtual machine.

5. For the **Name** field, enter a name for the new virtual machine.

6. Under **Instance Images**, add storage to the virtual machine by either using an existing virtual disk or creating a new virtual disk.

   - To use an existing virtual disk, click **Attach** and select the virtual disk to use for the virtual machine storage. Then click **OK**.

   - To create a new virtual disk, click **Create** and update the fields for the virtual machine storage or accept the default settings. Then click **OK**.

   The following screenshot shows the **New Virtual Disk** dialog box for the Oracle Linux virtual machine being created in this example scenario. In the dialog box, the following key fields are completed:

   - For the **Size (GiB)** field, a value of **12** is entered.

   - From the **Interface** drop-down list, **IDE** is selected.

   - From the **Allocation Policy** drop-down list, **Thin Provision** is selected.
7. Connect the virtual machine to a network by selecting the vNIC profile created in Creating a Logical Network from the nic1 drop-down list.

For information about customizing vNICs, refer to Customizing vNIC Profiles for Virtual Machines.

The following screenshot shows the General tab on New Virtual Machine dialog box for the new Microsoft Windows virtual machine that is being created in this example scenario. In the dialog box, the following key fields are completed:

- From the Cluster drop-down list, the Default option is selected.
- For the Operating System drop-down list, Windows 10 x64 is selected.
- For the Name field, windows-10-vm is entered.
- Under Instance Images, a virtual disk named windows-10-vm_Disk1 is being created, which has been set to a size of 12GB.
- From the nic1 drop-down list, the logical network named vm_pub is selected.
8. Click the **System** tab on the sidebar to adjust the memory size for the virtual machine from the defaults. In this example, change the **Memory Size** field to **4096 MB** and the **Total Virtual CPUs** field to **4**.

The following screenshot shows the **System** tab on **New Virtual Machine** dialog box for the new Microsoft Windows virtual machine that is being created in this example scenario. In the dialog box, the following key fields are completed:

- The **Memory Size** field is changed to **4096 MB**.
- The **Maximum memory** field automatically updates to **16384 MB** when the **Memory Size** field is changed to **4096 MB**.
- The **Total Virtual CPUs** field is changed to **4**.
9. Click the **Boot Options** tab on the sidebar of the dialog box to specify the boot sequence for the virtual device.

   a. From the **First Device** drop-down list select **CD-ROM**.

   b. Select the **Attach CD** checkbox and choose the appropriate ISO image from the drop-down list.

   After you install the Microsoft Windows guest OS, change the **First Device** drop-down list from **CD-ROM** to **Hard Disk** from the drop-down list. For more information, refer to Installing the Microsoft Windows Guest Agent and VirtIO Drivers.

   In the following screenshot, **CD-ROM** is selected from the **First Device** drop-down list. The **Attach CD** check box is also selected with the **en_windows_10_enterprise_1511_x64_dvd.iso** ISO file chosen from the drop-down list.
10. Click OK to create the virtual machine.

11. Proceed to Installing the Oracle Linux Guest OS.

Installing the Microsoft Windows Guest OS

To install the Microsoft Windows guest OS:

1. Go to Compute and then click Virtual Machines.

   The Virtual Machines pane opens with the list of virtual machines that have been created.

2. Select the Microsoft Windows virtual machine created in Creating a New Microsoft Windows Virtual Machine and click Run.

3. Click Console to open a console to the virtual machine.

   If you have not installed the Remote Viewer application, refer to Chapter 1, Before You Begin.

4. Install the Microsoft Windows guest OS.
Refer to the applicable Microsoft Windows documentation for instructions on how to install the operating system.

5. Proceed to Installing the Microsoft Windows Guest Agent and VirtIO Drivers.

**Installing the Microsoft Windows Guest Agent and VirtIO Drivers**

To install the Microsoft Windows guest agent and VirtIO drivers:

1. After you finish installing the Microsoft Windows guest OS, return to the Virtual Machines pane, highlight the row for this virtual machine, and click **Edit**.

   The **Edit Virtual Machines** dialog box opens.

2. Click the **Boot Options** tab on the sidebar of the dialog box to specify the boot sequence for the virtual device.

   a. From the **First Device** drop-down list, change **CD-ROM** to **Hard Disk**.
   
   b. From the **Second Device** drop-down list, select **CD-ROM**.
   
   c. Select the **Attach CD** checkbox and choose **oVirt-toolsSetup_4.2-4.el7.iso** from the drop-down list.

3. Click **OK** to save the changes to the virtual machine configuration.

4. Click **OK** when the **Pending Virtual Machine changes** dialog box appears.

5. From the **Virtual Machines** pane, reboot the virtual machine.

6. Click **Console** to open a console to the virtual machine and navigate to the CDROM.

7. Double-click **ovirt-guest-tools-setup** to install the Microsoft Windows guest agent.

8. Double-click the **virtio** folder and then click **Setup** to start the Oracle VirtIO Drivers for Microsoft Windows installer.

   The installer window is displayed.

9. Click **Install** to start the Oracle VirtIO Drivers for Microsoft Windows installer.

   The installer copies the Oracle VirtIO Drivers for Microsoft Windows installer files and then installs the drivers on the Microsoft Microsoft Windows guest OS.

10. Click **Yes, I want to restart my computer now** and click **Finish**.

    The virtual machine is restarted.

11. Stop the virtual machine.

12. Go to **Compute** and then click **Virtual Machines**.

    The **Virtual Machines** pane opens with the list of virtual machines that have been created.

13. Select the Microsoft Windows virtual machine created in *Creating a New Microsoft Windows Virtual Machine* and click **Edit**.

14. Edit the virtual disk. From the **Interface** drop-down list, change **IDE** to **VirtIO-SCSI**.
Creating a Template

15. Click the **Boot Options** tab on the sidebar.
   
a. Do not make any changes to the **First Device** drop-down list. The **Hard Disk** option is selected from a previous step.
   
b. From the **Second Device** drop-down list, select **None**.
   
c. Deselect the **Attach CD** checkbox.

16. Click **OK** to save the changes to the virtual machine configuration.

17. Run the Microsoft Windows virtual machine.

Creating a Template

For this example scenario, you seal the Oracle Linux virtual machine created in **Creating a New Virtual Machine** and then you create an Oracle Linux template based on that virtual machine. You then use that template as the basis for a Cloud-Init enabled template to automate the initial setup of a virtual machine.

A template is a copy of a virtual machine that you can use to simplify the subsequent, repeated creation of similar virtual machines. Templates capture the configuration of software, the configuration of hardware, and the software installed on the virtual machine on which the template is based, which is known as the source virtual machine.

Virtual machines that are created based on a template use the same NIC type and driver as the original virtual machine but are assigned separate, unique MAC addresses.

Sealing an Oracle Linux Virtual Machine for Use as a Template

Sealing is the process of removing all system-specific details from a virtual machine before creating a template based on that virtual machine. Sealing is necessary to prevent the same details from appearing on multiple virtual machines that are created based on the same template. It is also necessary to ensure the functionality of other features, such as predictable vNIC order.

To seal an Oracle Linux virtual machine for use as a template:

1. Log in to the Oracle Linux virtual machine as the **root** user.

2. Flag the system for reconfiguration.

   ```bash
   touch /.unconfigured
   ``

3. Remove the SSH host keys.

   ```bash
   rm -rf /etc/ssh/ssh_host_*
   ```

4. Set the host name value of the **HOSTNAME=localhost.localdomain** in the `/etc/sysconfig/network` file for Oracle Linux 6 or the `/etc/hostname` file for Oracle Linux 7.

5. Remove `/etc/udev/rules.d/70-*`.

   ```bash
   rm -rf /etc/udev/rules.d/70-*
   ```

6. Remove the **HWADDR** and **UUID** lines in the `/etc/sysconfig/network-scripts/ifcfg-eth*` file.

7. **(Optional)** Delete all the logs from `/var/log` and build logs from `/root`.

8. Cleanup the command history.
9. Shutdown the virtual machine.

```
# poweroff
```

The Oracle Linux virtual machine is now sealed and ready to be made into a template.

Creating an Oracle Linux Template

When you create a template based on a virtual machine, a read-only copy of the virtual machine's disk is created. This read-only disk becomes the base disk image of the new template, and of any virtual machines that are created based on the template. As such, the template cannot be deleted while any virtual machines based on that template exist in the virtualization environment.

To create an Oracle Linux template:

1. Go to **Compute**, and then click **Virtual Machines**.

   The **Virtual Machines** pane opens with the list of virtual machines that have been created.

2. Click **More Actions** to expand the drop-down list and select **Make Template** from the drop-down list.

   The following screenshot shows the **More Actions** drop-down list expanded to display the **Make Template** option. The **Make Template** option is highlighted with a red rectangular box for emphasis.

   **Figure 2.12 Make Template Option**

3. For the **Name** field, enter a name for the new virtual machine template.

4. In the **Disc Allocation** section under the **Alias** column, rename the disk alias to be the same as the template name entered for the **Name** field.
5. Click the **Seal Template (Linux only)** checkbox.

The following screenshot shows the **New Template** dialog box completed for the new template named `ol7-vm-template`, which is being created in this example scenario. In the dialog box, the disk alias has been renamed to `ol7-vm-template` and the **Seal Template (Linux only)** checkbox is selected.

![Figure 2.13 New Template Dialog Box](image-url)

6. Click the **OK** button to create the template.

The virtual machine displays a status of image `Locked` while the template is being created. The time it takes for the template to be created depends on the size of the virtual disk and the capabilities of your storage hardware. When the template creation process completes, the template is added to the list of templates displayed on the **Templates** pane.

You can now create new Oracle Linux virtual machines that are based on this template.

**Creating a Cloud-Init Enabled Template**

For Oracle Linux 7 and later VMs, you can use the Cloud-Init tool to automate the initial setup of virtual machines. Common tasks, such as configuring host names, network interfaces, and authorized keys, can be automated by using this tool. When provisioning virtual machines that have been deployed based on a template, the Cloud-Init tool can be used to prevent conflicts on the network.
Creating a Cloud-Init Enabled Template

Before You Begin

Before you create Cloud-Init enabled templates, ensure the following prerequisites are met:

- To use Cloud-Init, the `cloud-init` package must first be installed on the virtual machine. Once installed, the Cloud-Init service starts during the boot process and searches for instructions on what to configure. You can use options in the Run Once window to provide these instructions on a one-time only basis, or use the options in the New Virtual Machine, Edit Virtual Machine, and Edit Template dialog boxes to provide these instructions every time the virtual machine starts.

- You must have sealed an Oracle Linux for use as a template. For more information, refer to Sealing an Oracle Linux Virtual Machine for Use as a Template.

- You must create a template. For more information, refer to Creating an Oracle Linux Template.

1. Log in to an Oracle Linux virtual machine.

2. List the `cloud-init` package.

   ```bash
   # yum list cloud-init
   ```

3. Install the `cloud-init` package.

   ```bash
   # yum install cloud-init
   ```

4. Run the following command to enable the `cloud-init` service.

   ```bash
   # systemctl enable cloud-init
   ```

5. Run the following command to start the `cloud-init` service.

   ```bash
   # systemctl start cloud-init
   ```

Using Cloud-Init to Automate the Initial Setup of a Virtual Machine

To use Cloud-Init to automate the initial setup of a virtual machine:

1. Go to Compute and then click Templates.

   The Templates pane opens with the list of templates that have been created.

2. Select a template and click the Edit button.

3. Click Show Advanced Options.

4. Click the Initial Run tab and select the Use Cloud-Init/Sysprep check box.

5. Enter a host name in the VM Hostname text field.

6. Select the Configure Time Zone check box and select a time zone from the Time Zone drop-down list.

7. Expand the Authentication section.

   - Select the Use already configured password check box to use the existing credentials, or clear that check box and enter a root password in the Password and Verify Password text fields to specify a new root password.

   - Enter any SSH keys to be added to the authorized hosts file on the virtual machine in the SSH Authorized Keys text area.

   - Select the Regenerate SSH Keys check box to regenerate SSH keys for the virtual machine.
8. Expand the **Networks** section.
   
   • Enter any DNS servers in the **DNS Servers** text field.
   
   • Enter any DNS search domains in the **DNS Search Domains** text field.
   
   • Select the **In-guest Network Interface** check box and use the **+ Add new** and **- Remove selected** buttons to add or remove network interfaces to or from the virtual machine.

   **Important**
   
   You must specify the correct network interface name and number (for example, `eth0`, `eno3`, `enp0s`); otherwise, the virtual machine's interface connection will be up but will not have the Cloud-Init network configuration.

9. Expand the **Custom Script** section and enter any custom scripts in the **Custom Script** text area.

---

**Creating a Virtual Machine from a Template**

For this example scenario, you create an Oracle Linux virtual machine from the template created in Creating a Template.

**Creating an Oracle Linux Virtual Machine from a Template**

To create an Oracle Linux virtual machine from a template:

1. Go to **Compute** and then click **Templates**.
   
   The **Templates** pane opens with the list of templates that have been created.

2. On the far right corner of the **Templates** pane, click **New VM**.
   
   The **New Virtual Machine** dialog box opens for the template.

3. On the **Cluster** drop-down list, select the data center and host cluster for the new host.
   
   By default, the **Default** option is selected in the drop-down list.

   For this step, leave **Default** selected from the drop-down list because the default data center and cluster are used in this example scenario.

   For the procedures to create new data centers or a new clusters, refer to Chapter 3, *Additional Administration Tasks*.

4. For the **Template** drop-down list, select the desired template from the drop-down list.
   
   For this example scenario, select the template created in Creating an Oracle Linux Template.

5. For the **Operating System** drop-down list, select the operating system from the drop-down list.

6. For the **Name** field, enter a name for the virtual machine.
   
   The following screenshot shows the **New Virtual Machine** dialog box for the new Oracle Linux virtual machine that is being created based on the template that was created in Creating an Oracle Linux Template. In the dialog box, the following key fields are completed:

   • From the **Cluster** drop-down list, the **Default** option is selected.
   
   • From the **Template** drop-down list, the template named `ol7-vm-template` is selected.
Creating an Oracle Linux Virtual Machine from a Template

- For the **Operating System** drop-down list, *Oracle Linux 7.x x64* is selected.
- For the **Name** field, *ol7-vm2* is entered.
- From the **nic1** drop-down list, the logical network named *vm_pub* is selected.

**Figure 2.14 New Virtual Machine Dialog Box for a Template - General Tab**

7. Click the **Boot Options** tab and ensure that the **First Device** is set to *Hard Disk*.

The following screenshot shows the **New Virtual Machines** dialog box with the **Boot Options** tab options selected for the new Oracle Linux virtual machine named *ol7-vm4* that is being created from the template named *ol7-vm-template* in this example. The **First Device** is set to *Hard Disk*.
8. Click **OK** to create the virtual machine from the template.

The new virtual machine appears on the **Virtual Machines** pane.

9. Highlight the virtual machine that you created from the template and then click **Run** to boot the virtual machine.

The red down arrow icon to the left of the virtual machine turns green and the **Status** column displays **Up** when the virtual machine is up and running on the network.

---

### Backing Up and Restoring the Manager

For this example scenario, you backup and restore the Oracle Linux Virtualization Manager by using the `engine-backup` command utility.

### Backing Up the Manager

To backup the Manager:

1. Log in to the host that is running the Manager.

---

Figure 2.15 New Virtual Machine Dialog Box for a Template - Boot Options Tab
2. Create a full backup of the Manager.

```
# engine-backup --mode=backup --scope=all --file=path --log=path
```

The following example shows how to use the `engine-backup` command to create a full backup of the Manager. A backup file and log file for the Manager backup is created in the path specified.

```
# engine-backup --mode=backup --scope=all --file=backup/file/ovirt-engine-backup --log=backup/log/ovirt-engine-backup.log
```

3. (Optional) Set up a `cron` job to take regular backups.

By default, the Manager does not take automatic backups. Oracle recommends that you take regular backups of the Manager.

The following example shows a sample `cron` job defined in a `crontab`-format file.

```
today=`date +'%Y%m%d-%H%M'`
engine-backup --mode=backup --scope=all --file=/backup/file/ovirt-engine-backup-$today
--log=/backup/log/ovirt-engine-backup-$today.log
```

### Restoring a Full Backup of the Manager

To restore a full backup of the Manager:

1. Log in to the host that is running the Manager.
2. Clean up the objects associated with the Manager.

```
# engine-cleanup
```

This `engine-cleanup` command removes the configuration files and cleans the database associated with the Manager.

The following example shows output from the `engine-cleanup` command.

```
  [ INFO ] Stage: Initializing
  [ INFO ] Stage: Environment setup
  Configuration files: ...
  Log file: ...
  Version: otopi-1.7.8 (otopi-1.7.8-1.el7)
  [ INFO ] Stage: Environment packages setup
  [ INFO ] Stage: Programs detection
  [ INFO ] Stage: Environment customization
  Do you want to remove all components? (Yes, No) [Yes]: Yes
  The following files were changed since setup:
  /etc/ovirt-engine/engine.conf.d/11-setup-sso.conf
  Remove them anyway? (Yes, No) [Yes]: Yes
  ---- PRODUCT OPTIONS ----
  [ INFO ] Stage: Setup validation
  During execution engine service will be stopped (OK, Cancel) [OK]: OK
  All the installed ovirt components are about to be removed ...(OK, Cancel)
  [Cancel]: OK
  [ INFO ] Stage: Transaction setup
```
3. Restore a full backup of the Manager.

The following form of the `engine-backup` command is used to a restore a full backup of the Manager.

```
engine-backup --mode=restore --scope=all --file=path --log=path --restore-permissions
```

The following example shows how to use the `engine-backup` command to restore a full backup of the Manager.

```
# engine-backup --mode=restore --scope=all --file=backup/file/ovirt-engine-backup --log=backup/log/ovirt-engine-backup.log
Preparing to restore:
- Unpacking file 'backup/file/ovirt-engine-backup'
Restoring:
- Files
  - Engine database 'engine'
  - Cleaning up temporary tables in engine database 'engine'
  - Updating DbJustRestored VdcOption in engine database
  - Resetting DwhCurrentlyRunning in dwh_history_timekeeping in engine database
  - Resetting HA VM status

Please note:

The engine database was backed up at 2019-03-25 12:48:02.000000000 -0700 .

Objects that were added, removed or changed after this date, such as virtual machines, disks, etc., are missing in the engine, and will probably require recovery or recreation.
```

DWH database 'ovirt_engine_history'
You should now run `engine-setup`.

Done.

4. Run the `engine-setup` command to complete the setup of the restored Manager.

```bash
# engine-setup
```

This command reconfigures the firewall and ensures that the Manager service is correctly configured.

5. Log in to the Manager and verify that the Manager has been restored to the backup.
Chapter 3 Additional Administration Tasks

Table of Contents

Global Configuration ........................................................................................................... 33
  Administering User Accounts from the Administration Portal ........................................ 33
  Administering User and Group Accounts from the Command Line ................................ 36
Data Centers ......................................................................................................................... 44
  Creating a New Data Center ............................................................................................ 44
Clusters .................................................................................................................................. 44
  Creating a New Cluster .................................................................................................... 44
Networks ................................................................................................................................. 46
  Customizing vNIC Profiles for Virtual Machines ............................................................ 46
Storage .................................................................................................................................... 47
  Preparing Local Storage for a KVM Compute Host ......................................................... 47
  Configuring a KVM Compute Host to Use Local Storage ................................................. 47
  Preparing NFS Storage .................................................................................................... 48
  Attaching an NFS Data Domain ....................................................................................... 49
  Adding an FC Data Domain ............................................................................................. 50
Virtual Machines ................................................................................................................... 50
  Live Editing a Virtual Machine ....................................................................................... 50
  Creating a Snapshot of a Virtual Machine ..................................................................... 52
  Restoring a Virtual Machine from a Snapshot ............................................................... 53
  Creating a Virtual Machine from a Snapshot ................................................................. 54
  Deleting a Snapshot ........................................................................................................ 54
  Migrating Virtual Machines between Hosts ..................................................................... 55
Encrypted Communication ..................................................................................................... 58
  Replacing the Oracle Linux Virtualization Manager Apache SSL Certificate ................ 58
Event Notifications .............................................................................................................. 60
  Configuring Event Notification Services on the Engine ................................................. 60
  Creating Event Notifications in the Administration Portal ............................................. 61
  Canceling Event Notifications in the Administration Portal ......................................... 62
  Configuring the Engine to Send SNMP Traps ................................................................. 62

The following Oracle Linux Virtualization Manager administration tasks are provided as a supplement to the Getting Started scenario (see Chapter 2, Getting Started with Oracle Linux Virtualization Manager).

For conceptual information about these topics, refer to Oracle Linux Virtualization Manager Architecture and Planning Guide.

Global Configuration

Global configuration options are set from the Configure dialog box. This dialog box is accessed by selecting Administration and then clicking Configure. From the Configure dialog box, you can configure a number of global resources for your virtualization environment, such as users, roles, system permissions, scheduling policies, instance types, and MAC address pools. You can also customize the way in which users interact with resources in the environment and configure options that can be applied to multiple clusters from a central location.

Administering User Accounts from the Administration Portal

The following tasks describe common user administration tasks that are performed in the Administration Portal.
Adding VM Portal Permissions to a User

Users must be created already before they can be added and assigned roles and permissions. For more information, refer to Administering User and Group Accounts from the Command Line.

In the following example procedure, a user is assigned the roles and permissions associated with the UserRole. This role gives the user the permission to log in to the VM Portal and to start creating virtual machines. The procedure also applies to group accounts.

1. Click Administration and then select Configure.

   The Configure dialog box opens with the Roles tab selected on the sidebar menu.

2. Click the System Permissions tab on the sidebar.

3. Click Add.

   The Add System Permission to User dialog box opens.

4. Select a profile from the Search drop-down list and click Go.

5. Select the check box next to the user or group account.

6. Under the Role to Assign drop-down list, select UserRole.

7. Click OK.

8. (Optional) Log in to the VM Portal to verify the permissions of the user account.

Removing Users and Groups

To use the Administration Portal to remove a user or group:

1. Go to Administration and then click Users.

   The Users pane opens.

2. On the Users pane, select either the User or Group tab to display the added users or groups.

3. Select the user or group to be removed.

4. Click Remove.

   The Remove User(s) dialog box opens.

5. Click OK to confirm the removal of the user.

   The user or group is removed and no longer appears on the Users pane.

Assigning Permissions to Users and Groups

Users and groups must be created already before they can be assigned roles and permissions. For more information, refer to Administering User and Group Accounts from the Command Line.

1. Go to Administration and then click Users.

   The Users pane opens.

2. Click Add.

   The Add Users and Groups dialog box opens.
3. Select either the **Users** option.
4. In the **Search** field, enter the name of the user or group to be added and then select **Go**.

   The dialog box updates to display the search results.
5. Select the check box next to the user or group to be added.
6. Click **Add**.

   The user or group is added and appears on the **Users** pane.
7. On the **Users** pane, select either the **User** or **Group** tab to display the added users or groups.
8. Display the detailed view for the user or group by clicking the name of the user under the **User Name** column or the name of the group under the **Group Name** column.
9. Click the **Permissions** tab.
10. Click **Add System Permissions**.

   The **Add System Permission to User** dialog box opens.
11. From the **Add System Permission to User** drop-down list, select the role to assign to the user.

### Creating a Custom Role

If you require a role that is not available in the default set of roles provided by the Manager, you can create a custom role.

**Note**

For more information about the default set of roles provided by the Manager, refer to the latest oVirt upstream documentation that is available at:

https://ovirt.org/documentation/

To create a custom role:

1. Click **Administration** and then select **Configure**.

   The **Configure** dialog box opens with the **Roles** tab selected on the sidebar menu. The **Roles** tab displays a list of administrator and user roles, and any custom roles that have been created.
2. Click **New**.

   The **New Role** dialog box opens.
3. For the **Name** and **Description** fields, enter an appropriate name and description for the role.
4. Under **Account Type**, select either **Admin** or **User**.
5. Under **Check Boxes to Allow Action**, select the appropriate objects whose permissions to assign to the user.

   Click **Expand All** to see the objects under each permissions group. Click **Collapse All** to collapse the list of objects under each of the permission group.
6. For each of the objects, select or clear the objects the actions to be permitted or denied for the custom role that is being created.
7. Click **OK** to create the custom role.

The custom role now appears on the **Roles** tab.

### Administering User and Group Accounts from the Command Line

The following sections describe the common tasks that can be performed to administer user accounts using the `ovirt-aaa-jdbc-tool` command utility. This utility is used to manage user and group accounts on the internal domain. To view a list all available options for managing user and group accounts, run the `ovirt-aaa-jdbc-tool --help` command.

**Note**

Changes made using `ovirt-aaa-jdbc-tool` command utility take effect immediately and do not require you to restart the Manager.

### Creating a New User Account

The `ovirt-aaa-jdbc-tool user add` command is used to create user accounts.

To create a new user account:

1. Log in to the host that is running the Manager.

2. Create a new user account.

   ```
   ovirt-aaa-jdbc-tool user add username option
   ```

   To view a full list of options available for creating a user account, run the `ovirt-aaa-jdbc-tool user add --help` command.

   The following example shows how to create a new user account and add a first and last name to associate with the account.

   ```
   # ovirt-aaa-jdbc-tool user add test1 --attribute=firstName=John --attribute=lastName=Doe
   adding user test1...
   user added successfully
   **Note**: by default created user cannot log in. see: `/usr/bin/ovirt-aaa-jdbc-tool user password-reset --help`
   ```

**Note**

After creating a new user account, you must set a password so that the user can log in. See **Setting the Password for a User Account**.

3. Add the newly created user in the Administration Portal and assign the group appropriate roles and permissions. See **Assigning Permissions to Users and Groups**.

### Setting the Password for a User Account

The `ovirt-aaa-jdbc-tool password-reset` command is used to set (or reset) passwords for a user account.

To set (or reset) the password for a user account:

1. Log in to the host that is running the Manager.

2. Set (or reset) the password for a user account.

   ```
   ovirt-aaa-jdbc-tool user password-reset username --password-valid-to yyyy-MM-dd HH:mm:ssX
   ```
### Note

You must set a value for the `--password-valid-to` option; otherwise the password expiry time defaults to the time of the last login.

By default, the password policy for user accounts on the internal domain has the following restrictions:

- A user password must be a minimum length of 6 characters.
- When resetting a password, you cannot use the three previous passwords used for the user account.

For more information on the password policy and other default settings, run the `ovirt-aaa-jdbc-tool settings show` command.

The following example shows how to set a user password. In the example, `0800` stands for GMT minus 8 hours.

```
# ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-to="2025-08-01 12:00:00-0800"
Password:
Reenter password:
updating user test1...
user updated successfully
```

### Editing User Information

The `ovirt-aaa-jdbc-tool user edit` command is used to edit user information associated with a user account.

To edit user information:

1. Log in to the host that is running the Manager.
2. Edit the user account.

`ovirt-aaa-jdbc-tool user edit username option`

To view a full list of options available for editing user information, run the `ovirt-aaa-jdbc-tool user edit --help` command.

The following example shows how to edit a user account by adding an email address to associate with this user.

```
# ovirt-aaa-jdbc-tool user edit test1 --attribute=email=jdoe@example.com
updating user test1...
user updated successfully
```

### Viewing User Information

The `ovirt-aaa-jdbc-tool user show` command is used to display user information.

To view detailed user information:

1. Log in to the host that is running the Manager.
2. Display information about a user.

`ovirt-aaa-jdbc-tool user show username`

The following example shows how to view details about a user account.
Removing a User

The **ovirt-aaa-jdbc-tool user delete** command is used to remove a user.

To remove a user account:

1. Log in to the host that is running the Manager.
2. Remove a user.

   ovirt-aaa-jdbc-tool user delete *username*

The following example shows how to remove a user account.

   # ovirt-aaa-jdbc-tool user delete test1
   deleting user test1...
   user deleted successfully

Disabling User Accounts

You can disable users on the local domains, including the internal **admin** user created that is created when you run the **engine-setup** command.

**Important**

Make sure you have at least one user in the environment with full administrative permissions before disabling the default internal administrative user account (**admin** user). The **SuperUser** role gives a user full administrative permissions.

To disable a user:

1. Log in to the host that is running the Manager.
2. Disable the user.

   ovirt-aaa-jdbc-tool user edit *username* --flag=+disabled

The following example shows how to disable the **admin** user.

   # ovirt-aaa-jdbc-tool user edit admin --flag=+disabled
   updating user admin...
Creating Group Accounts

The `ovirt-aaa-jdbc-tool` command is used to create and manage group accounts on the internal domain. Managing group accounts is similar to managing user accounts. To view all available options for managing group accounts, run the `ovirt-aaa-jdbc-tool group --help` command. Common examples are provided in this section.

Creating a Group

To create a group account:

1. Log in to the host that is running the Manager.

2. Create a new group account.

   ```bash
   ovirt-aaa-jdbc-tool group add group-name
   ```

   **Note**
   Users must be created before they can be added to groups.

   The following examples shows how to add a new group account.

   ```bash
   # ovirt-aaa-jdbc-tool group add group1
   adding group group1...
   group added successfully
   ```

3. Add users to the group:

   ```bash
   ovirt-aaa-jdbc-tool group-manage useradd group-name --user=username
   ```

   To view a full list of the options for adding or removing members to and from groups, run the `ovirt-aaa-jdbc-tool group-manage --help` command.

   The following example shows how to add users to a group.

   ```bash
   # ovirt-aaa-jdbc-tool group-manage useradd group1 --user test1
   updating user group1...
   user updated successfully
   ```

4. Display group account details.

   ```bash
   ovirt-aaa-jdbc-tool group show group-name
   ```

   The following example shows how to display details about a group account.

   ```bash
   # ovirt-aaa-jdbc-tool group show group1
   -- Group group1(f23ca27c-1d6a-4f6e-8c3e-1e03e8e56829) --
   Namespace: *
   Name: group1
   ID: f23ca27c-1d6a-4f6e-8c3e-1e03e8e56829
   Display Name: 
   Description:
   ```
5. Add the newly created group in the Administration Portal and assign the group appropriate roles and permissions. See Assigning Permissions to Users and Groups.

The users in the group inherit the roles and permissions of the group.

**Creating Nested Groups**

To create nested groups:

1. Log in to the host that is running the Manager.

2. Create the first group account.

   ```
   ovirt-aaa-jdbc-tool group add group1
   ```

   The following examples shows how to add a new group account.

   ```
   # ovirt-aaa-jdbc-tool group add group1
   adding group group1...
   group added successfully
   ```

3. Create the second group account.

   ```
   ovirt-aaa-jdbc-tool group add group2
   ```

   The following examples shows how to create the second group account.

   ```
   # ovirt-aaa-jdbc-tool group add group2
   adding group group2...
   group added successfully
   ```

4. Add the second group to the first group.

   ```
   ovirt-aaa-jdbc-tool group manage group add group1 --group=group2
   ```

   The following examples shows how to add the second group to the first group.

   ```
   # ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group2
   updating group group1...
   group updated successfully
   ```

5. Add the first group in the Administration Portal and assign the group appropriate roles and permissions. See Assigning Permissions to Users and Groups.

**Removing a Group Account**

To remove a group account:

1. Log in to the host that is running the Manager.

2. Remove a group account.

   ```
   ovirt-aaa-jdbc-tool group delete group-name
   ```

   The following example shows how to remove a group account.

   ```
   # ovirt-aaa-jdbc-tool group delete group3
   deleting group group3...
   ```
Querying Users and Groups

The `ovirt-aaa-jdbc-tool query` command is used to query user and group information. To view a full list of options available for querying users and groups, run the `ovirt-aaa-jdbc-tool query --help` command.

Listing All User or Group Account Details

To list all account information:

1. Log in to the host that is running the Manager.
2. Display account details.

   • List all user user account details.

```
   ovirt-aaa-jdbc-tool query --what=user
```

The following example shows sample output from the `ovirt-aaa-jdbc-tool query --what=user` command.

```
# ovirt-aaa-jdbc-tool query --what=user
-- User test2(35e8b35e-2320-45da-b59e-1076b521d13f) --
Namespace: *
Name: test2
ID: 35e8b35e-2320-45da-b59e-1076b521d13f
Display Name: 
Email: 
First Name: Jane
Last Name: Doe
Department: 
Title: 
Description: 
Account Disabled: false
Account Locked: false
Account Unlocked At: 1970-01-01 00:00:00Z
Account Valid From: 2019-09-06 16:51:32Z
Account Valid To: 2219-09-06 16:51:32Z
Account Without Password: false
Last successful Login At: 2019-09-06 17:12:08Z
Last unsuccessful Login At: 1970-01-01 00:00:00Z
Password Valid To: 2025-08-01 20:00:00Z
-- User admin(89559d7f-3b48-420b-bd4d-2790122c199b) --
Namespace: *
Name: admin
ID: 89559d7f-3b48-420b-bd4d-2790122c199b
Display Name: 
Email: 
First Name: admin
Last Name: 
Department: 
Title: 
Description: 
Account Disabled: false
Account Locked: false
Account Unlocked At: 2019-03-07 11:09:07Z
Account Valid To: 2219-01-24 21:18:11Z
Account Without Password: false
Last successful Login At: 2019-09-06 18:10:11Z
Last unsuccessful Login At: 2019-09-06 18:09:36Z
Password Valid To: 2025-08-01 20:00:00Z
-- User test1(e75956a8-6ebf-49d7-94fa-504afbf96ad) --
Namespace: *
Name: test1
```
• List all group account details.

`ovirt-aaa-jdbc-tool query --what=group`

The following example shows sample output from the `ovirt-aaa-jdbc-tool query --what=group` command.

```
# ovirt-aaa-jdbc-tool query --what=group
-- Group group2(d6e0b913-d038-413a-b732-bc0c33ea1ed4) --
Namespace: *
Name: group2
ID: d6e0b913-d038-413a-b732-bc0c33ea1ed4
Display Name: 
Description: 
-- Group group1-1(e43ba527-6256-4c29-bd7a-0fb08b990b72) --
Namespace: *
Name: group1-1
ID: e43ba527-6256-4c29-bd7a-0fb08b990b72
Display Name: 
Description: 
-- Group group1(f23ca27c-1d6a-4f6e-8c3e-1e03e8e56829) --
Namespace: *
Name: group1
ID: f23ca27c-1d6a-4f6e-8c3e-1e03e8e56829
Display Name: 
Description: 
```

Listing Filtered Account Details

To apply filters when listing account information:

1. Log in to the host that is running the Manager.
2. Filter account details using the `--pattern` keyword.

• List user account based on a pattern.

`ovirt-aaa-jdbc-tool query --what=user --pattern=attribute=value`

The following example shows how to filter the output of the `ovirt-aaa-jdbc-tool query` command to display only user account details that start with the character J.

```
# ovirt-aaa-jdbc-tool query --what=user --pattern="firstName=J*
-- User test1(e75956a8-6ebf-49d7-94fa-504afbf96ad) --
Namespace: *
Name: test1
ID: e75956a8-6ebf-49d7-94fa-504afbf96ad
```
Display Name:
Email: jdoe@example.com
First Name: John
Last Name: Doe
Department:
Title:
Description:
Account Disabled: false
Account Locked: false
Account Unlocked At: 1970-01-01 00:00:00Z
Account Valid From: 2019-08-29 18:15:20Z
Account Valid To: 2219-08-29 18:15:20Z
Account Without Password: false
Last successful Login At: 1970-01-01 00:00:00Z
Last unsuccessful Login At: 1970-01-01 00:00:00Z
Password Valid To: 2025-08-01 20:00:00Z

-- User test2(35e8b35e-2320-45da-b59e-1076b521d13f) --
Namespace: *
Name: test2
ID: 35e8b35e-2320-45da-b59e-1076b521d13f
Display Name:
Email:
First Name: Jane
Last Name: Doe
Department:
Title:
Description:
Account Disabled: false
Account Locked: false
Account Unlocked At: 1970-01-01 00:00:00Z
Account Valid From: 2019-09-06 16:51:32Z
Account Valid To: 2219-09-06 16:51:32Z
Account Without Password: false
Last successful Login At: 2019-09-06 17:12:08Z
Last unsuccessful Login At: 1970-01-01 00:00:00Z
Password Valid To: 2025-08-01 20:00:00Z

• List groups based on a pattern.

ovirt-aaa-jdbc-tool-query --what=group --pattern=attribute=value

The following example shows how to filter the output of the ovirt-aaa-jdbc-tool query command to display only group account details that match the description documentation-group.

# ovirt-aaa-jdbc-tool query --what=group --pattern="description=documentation-group"

Managing Account Settings

The ovirt-aaa-jdbc-tool settings command is used to change the default account settings.

To change the default account settings:

1. Log in to the host that is running the Manager.
2. (Optional) Display all the settings that are available.

ovirt-aaa-jdbc-tool setting show
Data Centers

Oracle Linux Virtualization Manager creates a default data center during installation. You can configure the default data center, or set up new appropriately named data centers.

A data center requires a functioning cluster, host, and storage domain to operate in your virtualization environment.

Creating a New Data Center

To create a new data center:

1. Go to **Compute** and then select **Data Centers**.

   The **Data Centers** pane opens.

2. Click **New**.

3. Select the storage **Type**, **Compatibility Version**, and **Quota Mode** of the data center from the respective drop-down menus.

4. Click **OK** to create the data center.

   The new data center is added to the virtualization environment and the **Data Center - Guide Me** menu opens to guide you through the entities that are required be configured for the data center to operate.

   The new data center remains in **Uninitialized** state until a cluster, host, and storage domain are configured for it.

   You can postpone the configuration of these entities by clicking the **Configure Later** button. You can resume the configuration of these entities by selecting the respective data center and clicking **More Actions** and then choosing **Guide Me** from the drop-down menu.

Clusters

Oracle Linux Virtualization Manager creates a default cluster in the default data center during installation. You can configure the default cluster, or set up new appropriately named clusters.

Creating a New Cluster

To create a new cluster:

1. Go to **Compute** and then select **Clusters**.

   The **Clusters** pane opens.

2. Click **New**.

   The **New Cluster** dialog box opens with the **General** tab selected on the sidebar.

3. From the **Data Center** drop-down list, choose the Data Center to associate with the cluster.
Creating a New Cluster

4. For the **Name** field, enter an appropriate name for the data center.

5. For the **Description** field, enter an appropriate description for the cluster.

6. From the **Management Network** drop-down list, choose the network for which to assign the management network role.

7. From the **CPU Architecture** and **CPU Type** drop-down lists, choose the CPU processor family and minimum CPU processor that match the hosts that are to be added to the cluster.

   For both Intel and AMD CPU types, the listed CPU models are in logical order from the oldest to the newest. If your cluster includes hosts with different CPU models, choose the oldest CPU model from the list to ensure that all hosts can operate in the cluster.

8. From the **Compatibility Version** drop-down list, choose the compatibility version of the cluster.

9. From the **Switch Type** drop-down list, choose the type of switch to be used for the cluster.

   By default, **Linux Bridge** is selected from the drop-down list.

10. From the **Firewall Type** drop-down list, choose the firewall type for hosts in the cluster.

    The firewall types available are either **iptables** or **firewalld**. By default, the **firewalld** option is selected from the drop-down list.

11. The **Enable Virt Service** check box is selected by default. This check box designates that the cluster is to be populated with virtual machine hosts.

12. *(Optional)* Select the **Enable to set VM maintenance reason** check box to enable an optional reason field when a virtual machine is shut down from the Administration Portal.

    You can use this field to provide an explanation for the maintenance window.

13. *(Optional)* Select the **Enable to set Host maintenance reason** check box to enable an optional reason field when a host is placed into maintenance mode from the Administration Portal.

    You can use this field to provide an explanation for the maintenance window.

14. *(Optional)* Review the other tabs to further configure your cluster:
   a. Click the **Optimization** tab on the sidebar to select the memory page sharing threshold for the cluster, and optionally enable CPU thread handling and memory ballooning on the hosts in the cluster. See Chapter 4, *Deployment Optimization*.
   b. Click the **Migration Policy** tab on the sidebar menu to define the virtual machine migration policy for the cluster.
   c. Click the **Scheduling Policy** tab on the sidebar to optionally configure a scheduling policy, configure scheduler optimization settings, enable trusted service for hosts in the cluster, enable HA Reservation, and add a custom serial number policy.
   d. Click the **Fencing policy** tab on the sidebar to enable or disable fencing in the cluster, and select fencing options.
   e. Click the **MAC Address Pool** tab on the sidebar to specify a MAC address pool other than the default pool for the cluster.

15. Click **OK** to create the data center.
The cluster is added to the virtualization environment and the **Cluster - Guide Me** menu opens to guide you through the entities that are required to be configured for the cluster to operate.

You can postpone the configuration of these entities by clicking the **Configure Later** button. You can resume the configuration of these entities by selecting the respective cluster and clicking **More Actions** and then choosing **Guide Me** from the drop-down menu.

**Networks**

With Oracle Linux Virtualization Manager, you can create custom vNICs for your virtual machines.

**Customizing vNIC Profiles for Virtual Machines**

To customize vNICs for virtual machines:

1. **Go to Compute and then click Virtual Machines.**
   - The **Virtual Machines** pane opens with the list of virtual machines that have been created.

2. **Under the Name column, select the virtual machine for which to add the virtual machine network.**
   - The **General** tab opens with details about the virtual machine.

3. **Click the Network Interfaces tab.**
   - The **Network Interfaces** tab opens with the available network interface to be used for the network.

4. **Highlight the network interface by clicking the row for the respective interface and then click Edit on the right side above the interface listing.**
   - The **Edit Network Interface** dialog box opens.

5. **In the Edit Network Interface dialog box, update the following fields:**
   - a. From the **Profile** drop-down list, select the network to be added to the virtual machine.
   - b. Click the **Custom MAC address** check box, and then enter or update the MAC address that is allocated for this virtual machine in the text entry field.

6. **Click OK when you are finished editing the network interface settings for the virtual machine.**

7. **Go to Compute and then click Virtual Machines.**
   - The **Virtual Machines** pane opens.

   **Important**

   Since virtual machines can start on any host in a data center/cluster, all hosts must have the customized VM network assigned to one of its NICs. Ensure that you assign this customized VM network to each host before booting the virtual machine. For more information, see Assigning the Virtual Machine Network to a KVM Compute Host.

8. **Highlight the virtual machine where you added the network and then click Run to boot the virtual machine.**

   The red down arrow icon to the left of the virtual machine turns green and the **Status** column displays **UP** when the virtual machine is up and running on the network.
Storage

Oracle Linux Virtualization Manager uses a centralized storage system for virtual machine disk images, ISO files, and snapshots. You can use Network File System (NFS), Internet Small Computer System Interface (iSCSI), or Fibre Channel Protocol (FCP) storage. You can also configure local storage attached directly to hosts.

This following administration tasks cover preparing and adding local, NFS, and FCP storage. For information about attaching iSCSI storage, refer to Attaching an iSCSI Data Domain.

Preparing Local Storage for a KVM Compute Host

Before you begin, ensure the following prerequisites have been met:

- You have allocated disk space for local storage. You can allocate an entire physical disk on the host or you can use a portion of the disk.

- You have created a filesystem on the block device path to be used for local storage. Local storage should always be defined on a file system that is separate from the root directory (/root).

To prepare local storage for a KVM compute host:

1. Create the directory to be used for the local storage on the host.

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

2. Ensure that the directory has permissions that allows read-write access to the vdsm user (UID 36) and kvm group (GID 36).

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

   The local storage can now be added to your virtualization environment.

Configuring a KVM Compute Host to Use Local Storage

When you configure a KVM compute host to use local storage, it is automatically added to a new data center and cluster that can contain no other hosts. With local storage, features, such as live migration, fencing, and scheduling, are not available.

To configure a KVM compute host to use local storage:

1. Go to Compute, and then click Hosts.

   The Hosts pane opens.

2. Highlight the host on which to add the local storage domain.

3. Click Management and then select Maintenance from the drop-down list.

   The Status column for the host displays Maintenance when the host has successfully entered into Maintenance mode.

4. After the host is in Maintenance mode, click Management and then select Configure Local Storage from the drop-down list.

   The Configure Local Storage pane opens with the General tab selected.
5. Click **Edit** next to the **Data Center**, **Cluster**, and **Storage** fields to configure and name the local storage domain.

6. In the **Set the path to your local storage** text input field, specify the path to your local storage domain.

   For more information, refer to **Preparing Local Storage for a KVM Compute Host**.

7. Click **OK** to add the local storage domain.

   When the virtualization environment is finished adding the local storage, the new data center, cluster, and storage created for the local storage appears on the **Data Center**, **Clusters**, and **Storage** panes, respectively.

   You can click **Tasks** to monitor the various processing steps that are completed to add the local storage to the host.

   You can also verify the successful addition of the local storage domain by viewing the `/var/log/ovirt-engine/engine.log` file.

---

### Preparing NFS Storage

Before preparing the NFS share, ensure your environment meets the following conditions:

- Ensure that the Manager and KVM host installation are running the latest Oracle Linux 7 Update 6 in an environment with two or more servers where one acts as the Manager host and the other servers act as KVM hosts.

  The installation creates a `vdsm:kvm (36:36)` user and group in the `/etc/passwd` and `/etc/group` directories, respectively.

  ```bash
  # cat /etc/passwd | grep vdsm
  vdsm:x:36:36:Node Virtualization Manager:/sbin/nologin
  
  # cat /etc/group | grep kvm
  kvm:x:36:qemu,sanlock
  ```

- An Oracle Linux NFS File server that is reachable by your virtualization environment.

To prepare NFS storage:

1. On a Linux fileserver that has access to the virtualization environment, create a directory that is to be used for the data domain.

   ```bash
   # mkdir -p /nfs/olv_ovirt/data
   ```

2. Set the required permissions on the new directory to allow read-write access to the `vdsm` user (UID 36) and `kvm` group (GID 36).

   ```bash
   # chown -R 36:36 /nfs/olv_ovirt
   # chmod -R 0755 /nfs/olv_ovirt
   ```

3. Add an entry for the newly created NFS share in the `/etc/exports` directory on the NFS fileserver that uses the following format: `full-path-of-share-created *(rw,sync,no_subtree_check,all_squash,anonuid=36,anongid=36)`.

   For example:

   ```bash
   # vi /etc/exports
   ```
Attaching an NFS Data Domain

To attach an NFS data domain:

1. Go to Storage and then click Domains.

   The Storage Domains pane opens.

2. Click New Domain.

   The New Domain dialog box opens.

3. From the Data Center drop-down list, select the Data Center for which to attach the data domain.

4. From the Domain Function drop-down list, select Data. By default, the Data option is selected in the drop-down list.

5. From the Storage Type drop-down list, select NFS. By default, the NFS option is selected in the drop-down list.

   When NFS is selected for the Storage Type, the options that are applicable to this storage types (such as the required Export Path option) are displayed in the New Domain dialog box.

6. For the Host to Use drop-down list, select the host for which to attach the data domain.

7. For the Export Path option, enter the remote path to the NFS export to be used as the storage data domain in the text input field.

   The Export Path option must be entered in one of the following formats: IP:/pathname or FQDN:/pathname (for example, server.example.com:/nfs/olv_ovirt/data).

# added the following entry

/nfs/olv_ovirt/data *(rw, sync, no_subtree_check, all_squash, anonuid=36, anongid=36)
:wq

Verify that the entry has been added.

# grep "/nfs/olv_ovirt/data" /etc/exports
/nfs/olv_ovirt/data *(rw, sync, no_subtree_check, all_squash, anonuid=36, anongid=36)

If you do not want to export the domain share to all servers on the network (denoted by the * before the left parenthesis), you can specify each individual host in your virtualization environment by using the following format: /nfs/ol_ovirt/data hostname-or-ip-address (rw, sync, no_subtree_check, all_squash, anonuid=36, anongid=36).

For example:

/nfs/olv_ovirt/data hostname (rw, sync, no_subtree_check, all_squash, anonuid=36, anongid=36)

4. Export the NFS share.

   # exportfs -rv

5. Confirm that the added export is available to Oracle Linux Virtualization Manager hosts by using the following showmount commands on the NFS File Server.

   # showmount -e | grep pathname-to-domain-share-added
   # showmount | grep ip-address-of-host
Adding an FC Data Domain

The /pathname that you enter must be the same as the path that you created on the NFS file server for the data domain in Preparing NFS Storage.

8. Click OK to attach the NFS storage data domain.

For information about uploading images to the data domain, see Uploading Images to the Data Domain.

Adding an FC Data Domain

To add an FC data domain:

1. Go to Storage and then click Domains.

The Storage Domains pane opens.

2. On the Storage Domains pane, click the New Domain button.

The New Domain dialog box opens.

3. For the Name field, enter a name for the data domain.

4. From the Data Center drop-down list, select the Data Center for which to attach the data domain. By default, the Default option is selected in the drop-down list.

5. From the Domain Function drop-down list, select the domain function. By default, the Data option is selected in the drop-down list.

   For this step, leave Data as the domain function because you are creating a data domain in this example.

6. From the Storage Type drop-down list, select Fibre Channel.

7. For the Host to Use drop-down list, select the host for which to attach the data domain.

8. When Fibre Channel is selected for the Storage Type, the New Domain dialog box automatically displays the known targets with unused LUNs.

9. Click Add next to the LUN ID that is connect to the target.

10. (Optional) Configure the advanced parameters.

11. Click OK.

   You can click Tasks to monitor the various processing steps that are completed to attach the FC data domain to the data center.

Virtual Machines

Oracle Linux Virtualization Manager lets you perform basic administration of your virtual machines, including live editing, creating and using snapshots and live migration.

Live Editing a Virtual Machine

You can optionally change many settings for a VM while it is running.

1. From the Administration Portal, click Compute and then select Virtual Machines.

2. From the list of virtual machine, highlight its row and then click Edit.
3. On the bottom left of the Edit Virtual Machine window, click Show Advanced Options.
4. Change any of the following while the VM without restarting the VM.

Select the General tab, to modify:

• **Optimized for**

  You can select from three options:

  • **Desktop** - the VM has a sound card, uses an image (thin allocation), and is stateless.
  
  • **Server** - the VM does not have a sound card, uses a cloned disk image, and is not stateless. In contrast, virtual machines optimized to act as desktop machines.
  
  • **High Performance** - the VM is pre-configured with a set of suggested and recommended configuration settings for reaching the best efficiency.

• **Name**

  A VM's name must be unique within the data center. It must not contain any spaces and must contain at least one character from A-Z or 0-9. The maximum length is 255 characters.

  The name can be re-used in different data centers within Oracle Linux Virtualization Manager.

• **Description** and **Comment**

• **Delete Protection**

  If you want to make it impossible to delete a VM, check this box. If you later decide you want to delete the VM, remove the check.

• **Network Interfaces**

  Add or remove network interfaces or change the network of an existing NIC.

Select the System tab, to modify:

• **Memory Size**

  Use to hot plug virtual memory. For more information, see Hot Plugging Virtual Memory.

• **Virtual Sockets** (Under Advance Parameters)

  Use to hot plug CPUs to the VM. Do not assign more sockets to a VM than are present on its KVM host. For more information, see Hot Plugging vCPUs.

Select the Console tab, to modify:

• **Disable strict user checking**

  By default, strict checking is enabled allowing only one user to connect to the console of a VM until it has been rebooted. The exception is that a SuperUser can connect at any time and replace a existing connection. When a SuperUser has connected, no normal user can connect again until the VM is rebooted.
Creating a Snapshot of a Virtual Machine

Important

Check this box with caution because you can expose the previous user’s session to the new user.

Select the High Availability tab, to modify:

• Highly Available

Check this box if you want the VM to automatically live migrate to another host if its host crashes or becomes non-operational. Only VMs with high availability are restarted on another host. If the VM's host is manually shut down, the VM does not automatically live migrate to another host. For more information, see Configuring a Highly Available Virtual Machine.

Note

You are not able to check this box if on the Host tab you have selected either Allow manual migration only or Do not allow migration for the Migration mode. For a VM to be highly-available it must be possible for the engine to migrate the VM to another host when needed.

• Priority for Run/Migration Queue

Select the priority level (Low, Medium or High) for the VM to live migrate or restart on another host.

Select the Icon tab, to upload a new icon.

5. Click OK when you are finished with all tabs to save your changes.

Changes to any other settings are applied when you shut down and restart your VM. Until then, an orange icon displays to indicate pending changes.

Creating a Snapshot of a Virtual Machine

A snapshot is a view of a virtual machine’s operating system and applications on any or all available disks at a given point in time. You can take a snapshot of a virtual machine before you make a change to it that may have unintended consequences. If needed, you can use the snapshot to return the virtual machine to its previous state.

To create a snapshot of a virtual machine:

1. Click Compute and then select Virtual Machines.

The Virtual Machines pane opens with the list of virtual machines that have been created.

2. Under the Name column, select the virtual machine for which to take a snapshot.

The General tab opens with details about the virtual machine.

3. Click the Snapshots tab.

4. Click Create.

5. (Optional) For the Description field, enter a description for the snapshot.

6. (Optional) Select the Disks to include checkboxes. By default, all disks are selected.
Restoring a Virtual Machine from a Snapshot

Important
Not selecting a disk results in the creation of a partial snapshot of the virtual machine without a disk. Although a saved partial snapshot does not have a disk, you can still preview a partial snapshot to view the configuration of the virtual machine.

7. (Optional) Select the Save Memory check box to include the virtual machine’s memory in the snapshot. By default, this checkbox is selected.

8. Click OK to save the snapshot.

The virtual machine’s operating system and applications on the selected disks are stored in a snapshot that can be previewed or restored.

On the Snapshots pane, the Lock icon appears next to the snapshot as it is being created. Once complete, the icon changes to the Snapshot (camera) icon. You can then display details about the snapshot by selecting the General, Disks, Network Interfaces, and Installed Applications drop-down views.

Restoring a Virtual Machine from a Snapshot

A snapshot can be used to restore a virtual machine to its previous state.

Note
The virtual machine must be in a Down state before performing this task.

To restore a virtual machine from a snapshot:

1. Click Compute and then select Virtual Machines.
   
The Virtual Machines pane opens with the list of virtual machines that have been created.

2. Under the Name column, select the virtual machine that you want to restore from a snapshot.
   
The General tab opens with details about the virtual machine.

3. Click the Snapshots tab.

4. On the Snapshots pane, select the snapshot to be used to restore the virtual machine.

5. From the Preview drop-down list, select Custom.
   
On the Virtual Machines pane, the status of the virtual machine briefly changes to Image Locked before returning to Down.

On the Snapshots pane, the Preview (eye) icon appears next to the snapshot when the preview of the snapshot is completed.

6. Click Run to start the virtual machine.
   
The virtual machine runs using the disk image of the snapshot. You can preview the snapshot and verify the state of the virtual machine.

7. Click Shutdown to stop the virtual machine.
8. From the **Snapshot** pane, perform one of the following steps:
   a. Click **Commit** to permanently restore the virtual machine to the condition of the snapshot. Any subsequent snapshots are erased.
   b. Alternatively, click **Undo** to deactivate the snapshot and return the virtual machine to its previous state.

### Creating a Virtual Machine from a Snapshot

Before performing this task, you must create a snapshot of a virtual machine. For more information, refer to [Creating a Snapshot of a Virtual Machine](#).

To create a virtual machine from a snapshot:

1. Click **Compute** and then select **Virtual Machines**.
   
   The **Virtual Machines** pane opens with the list of virtual machines that have been created.

2. Under the **Name** column, select the virtual machine with the snapshot that you want to use as the basis from which to create another virtual machine.
   
   The **General** tab opens with details about the virtual machine.

3. Click the **Snapshots** tab.

4. On the **Snapshots** pane, select the snapshot from which to create the virtual machine.

5. Click **Clone**.
   
   The **Clone VM from Snapshot** dialog box opens.

6. For the **Name** field, enter a name for the virtual machine.

   **Note**
   
   The **Name** field is the only required field on this dialog box.

   After a short time, the cloned virtual machine appears on the **Virtual Machines** pane with a status of **Image Locked**. The virtual machine remains in this state until the Manager completes the creation of the virtual machine. When the virtual machine is ready to use, its status changes from **Image Locked** to **Down** on the **Virtual Machines** pane.

### Deleting a Snapshot

You can delete a virtual machine snapshot and permanently remove it from your virtualization environment. This operation is supported on a running virtual machine and does not require the virtual machine to be in a **Down** state.

**Important**

- When you delete a snapshot from an image chain, there must be enough free space in the storage domain to temporarily accommodate both the original volume and the newly merged volume; otherwise, the snapshot deletion fails. This is due to the data from the two volumes being merged in the resized volume and the resized volume growing to accommodate the total size of the two merged volumes.
Migrating Virtual Machines between Hosts

To delete a snapshot:

1. Click Compute and then select Virtual Machines.
   The Virtual Machines pane opens with the list of virtual machines that have been created.
2. Under the Name column, select the virtual machine with the snapshot that you want to delete.
   The General tab opens with details about the virtual machine.
3. Click the Snapshots tab.
4. On the Snapshots pane, select the snapshot to delete.
5. Select the snapshot to delete.
6. Click Delete.
7. Click OK.
   On the Snapshots pane, a Lock icon appears next to the snapshot until the snapshot is deleted.

Migrating Virtual Machines between Hosts

Live migration allows you to move a running VM between physical hosts with no interruption to service. The VM stays powered on and user applications continue running while the VM is relocated to a new physical host. In the background, the VM's RAM is copied from the source host to the destination host. Storage and network connectivity are not changed.

You use live migration to seamlessly move VMs to support a number of common maintenance tasks. Ensure that your environment is correctly configured to support live migration well in advance of using it.

Configuring Your Environment for Live Migration

To enable successful live migrations, you should ensure you correctly configure it. At a minimum, to successfully migrate running VMs:

- Source and destination hosts should be in the same cluster
- Source and destination hosts must have a status of Up.
- Source and destination hosts must have access to the same virtual networks and VLANs
- Source and destination hosts must have access to the data storage domain where the VMs reside
- There must be enough CPU capacity on the destination host to support the VMs requirements.
• There must be enough RAM on the destination host that is not in use to support the VMs requirements

**Note**

Live migrations are performed using the management network. Each live migration event is limited to a maximum transfer speed of 30 MBps, and the number of concurrent migrations supported is also limited by default. Even with these limits, concurrent migrations can potentially saturate the management network. To minimize the risk of network saturation, we recommend that you create separate logical networks for storage, display, and VM data.

To configure VMs so they reduce network outage during migration:

• Ensure that the destination host has an available virtual function (VF)

• Set the **Passthrough** and **Migrateable** options in the passthrough vNIC’s profile

• Enable hotplugging for the VM’s network interface

• Ensure that the VM has a backup VirtIO vNIC to maintain the VM’s network connection during migration

• Set the VirtIO vNIC’s **No Network Filter** option before configuring the bond

• Add both vNICs as slaves under an active-backup bond on the VM, with the passthrough vNIC as the primary interface

### Optimizing Live Migration

Live VM migration can be a resource-intensive operation. There are two options you can set globally for every VM in the environment, at the cluster level, or at the individual VM level to optimize live migration.

• Set the **Auto Converge migrations** option to use auto-convergence during live migration of VMs.

• Set the **Enable migration compression** option to use migration compression during live migration of the VM.

Both options are disabled globally by default.

To configure auto-convergence and migration compression for VM migration:

1. Log onto the Engine host from a terminal window.

2. Configure the optimization settings at the global level.

   a. Enable auto-convergence globally.

   ```bash
   # engine-config -s DefaultAutoConvergence=True
   ```

   b. Enable migration compression globally.

   ```bash
   # engine-config -s DefaultMigrationCompression=True
   ```

   c. Restart the `ovirt-engine` service to apply the changes.

   ```bash
   systemctl restart ovirt-engine.service
   ```

3. Configure the optimization settings at the cluster level.

   a. Click **Compute** and then select **Clusters**.
b. Select a Cluster and click Edit.

c. Click the Migration Policy tab.

d. Select Inherit from global setting, Auto Converge, or Don’t Auto Converge from the Auto Converge migrations drop-down list.

e. Select Inherit from global setting, Compress, or Don’t Compress from the Enable migration compression drop-down list.

f. Click OK.

4. Configure the optimization settings at the cluster level.

a. Click Compute and then select Virtual Machines.

b. Select a Virtual Machine and click Edit.

c. Click the Host tab.

d. Select Inherit from cluster setting, Auto Converge, or Don’t Auto Converge from the Auto Converge migrations drop-down list.

e. Select Inherit from cluster setting, Compress, or Don’t Compress from the Enable migration compression drop-down list.

f. Click OK.

Automatic Virtual Machine Migration

The Engine automatically initiates live migration of VMs in two situations:

• When a host is moved into maintenance mode live migration is initiated for all VMs running on the host. The destination host for each VM is assessed as the VM is migrated, in order to spread the load across the cluster.

• To maintain load balancing or power saving levels in line with scheduling policy live migrations are initiated.

You can disable automatic, or even manual, live migration of specific VMs if required.

Setting Virtual Machine Migration Mode

You can disable automatic migration of a VM and you can disable manual migration of a VM by setting the virtual machine to run only on a specific host.

To prevent automatic migration of a VM:

1. Click Compute and select Virtual Machines.

2. Select a virtual machine and click Edit.

3. Click the Host tab.

4. Use the Start Running On radio buttons to specify whether the VM should run on any host in the cluster, a specific host, or a group of hosts.
If the VM has host devices attached to it, and you choose a different host, the host devices from the previous host are removed from the VM.

**Warning**

Assigning a VM to one specific host and disabling migration is mutually exclusive in Oracle Linux Virtualization Manager high availability (HA). Virtual machines that are assigned to one specific host can only be made highly available using third-party HA products. This restriction does not apply to virtual machines that are assigned to a group of hosts.

5. From the **Migration mode** drop-down list, select **Allow manual and automatic migration**, **Allow manual migration only** or **Do not allow migration**.

If you want to use auto-convergence and migration compression, you must select **Allow manual and automatic migration**. See Optimizing Live Migration.

6. (Optional) Check **Use custom migration downtime** and specify a value in milliseconds.

7. Click **OK**.

### Manually Migrate a Virtual Machine

To manually migrate a VM:

1. Click **Compute** and select **Virtual Machines**.

2. Select a running VM and click **Migrate**.

3. Choose either **Select Host Automatically** or **Select Destination Host** and select the destination host from the drop-down list.

   When you choose **Select Host Automatically**, the system determines the destination host according to the load balancing and power management rules set up in the scheduling policy.

4. Click **OK**.

   During migration, progress is shown in the **Status** field. When the VM has been migrated, the **Host** field updates to show the VM's new host.

### Encrypted Communication

You can configure your organization’s third-party CA certificate to identify the Oracle Linux Virtualization Manager to users connecting over HTTPS.

Using a third-party CA certificate for HTTPS connections does not affect the certificate that is used for authentication between the engine host and KVM hosts. They continue to use the self-signed certificate generated by the Manager.

### Replacing the Oracle Linux Virtualization Manager Apache SSL Certificate

Before you begin, you must obtain a third-party CA certificate, which is a digital certificate issued by a certificate authority (CA). The certificate is provided as a PEM file. The certificate chain must be complete up to the root certificate. The chain’s order is critical and must be from the last intermediate certificate to the root certificate.
Replacing the Oracle Linux Virtualization Manager Apache SSL Certificate

Caution

Do not change the permissions and ownerships for the /etc/pki directory or any subdirectories. The permission for the /etc/pki and /etc/pki/ovirt-engine directories must remain as the default value of 755.

To replace the Oracle Linux Virtualization Manager Apache SSL Certificate:

1. Copy the new third-party CA certificate to the host-wide trust store and update the trust store.

   ```
   # cp third-party-ca-cert.pem /etc/pki/ca-trust/source/anchors/
   # update-ca-trust export
   ```

2. Remove the symbolic link to /etc/pki/ovirt-engine/apache-ca.pem.

   The Engine has been configured to use /etc/pki/ovirt-engine/apache-ca.pem, which is symbolically linked to /etc/pki/ovirt-engine/ca.pem.

   ```
   # rm /etc/pki/ovirt-engine/apache-ca.pem
   ```

3. Copy the CA certificate into the PKI directory for the Manager.

   ```
   cp third-party-ca-cert.pem /etc/pki/ovirt-engine/apache-ca.pem
   ```

4. Back up the existing private key and certificate.

   ```
   # cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-engine/keys/apache.key.nopass.bck
   # cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
   ```

5. Copy the new Apache private key into the PKI directory for the Manager by entering the following command and respond to prompt.

   ```
   # cp apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
   cp: overwrite /u2018/etc/pki/ovirt-engine/keys/apache.key.nopass\u2019? y
   ```

6. Copy the new Apache certificate into the PKI directory for the Manager by entering the following command and respond to the prompt.

   ```
   # cp apache.cer /etc/pki/ovirt-engine/certs/apache.cer
   cp: overwrite /u2018/etc/pki/ovirt-engine/certs/apache.cer\u2019? y
   ```

7. Restart the Apache HTTP server (httpd) and the Manager.

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

8. Create a new trust store configuration file (or edit the existing one) at /etc/ovirt-engine/ engine.conf.d/99-custom-truststore.conf by adding the following parameters.

   ```
   ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
   ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
   ```


   ```
   # cp /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf.bck
   ```

10. Edit the Websocket configuration file at /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf by adding the following parameters.

    ```
    SSL_CERTIFICATE="/etc/pki/ovirt-engine/apache.cer"
    ```
Event Notifications

The following section explains how to set up event notifications to monitor events in your virtualization environment. You can configure the Manager to send event notifications in email to alert designated users when certain events occur or enable Simple Network Management Protocol (SNMP) traps to monitor your virtualization environment.

Configuring Event Notification Services on the Engine

For event notifications to be sent properly to email recipients, you must configure the mail server on the Engine and enable `ovirt-engine-notifier` service. For more information about creating event notifications in the Administration portal, see Creating Event Notifications in the Administration Portal.

To configure notification services on the Engine:

1. Log in to the host that is running the Manager.
2. Copy the `ovirt-engine-notifier.conf` to a new file named `90-email-notify.conf`.

   ```bash
   ```

3. Edit the `90-email-notify.conf` file by deleting everything except the EMAIL Notifications section.

   ```
   # EMAIL Notifications
   
   # The SMTP mail server address. Required.
   MAIL_SERVER=myemailserver.mycompany.com
   
   # The SMTP port (usually 25 for plain SMTP, 465 for SMTP with SSL, 587 for SMTP with TLS)
   MAIL_PORT=25
   
   # Required if SSL or TLS enabled to authenticate the user. Used also to specify 'from' user address if mail server supports, when MAIL_FROM is not set. Address is in RFC822 format
   MAIL_USER=email.example.com
   
   # Required to authenticate the user if mail server requires authentication or if SSL or TLS is enabled
   SENSITIVE_KEYS="${SENSITIVE_KEYS},MAIL_PASSWORD"
   ```

Note

If you plan to also configure SNMP traps in your virtualization environment, you can also copy the values from the SNMP_TRAP Notifications section of the `ovirt-notifier.conf` file to a file named `20-snmp.conf`. For more information, see Configuring the Engine to Send SNMP Traps.

4. Enter the correct email variables. This file overrides the values in the original `ovirt-engine-notifier.conf` file.

11. Restart the `ovirt-provider-ovn` service.

   ```bash
   systemctl restart ovirt-provider-ovn
   ```

12. Restart the `ovirt-engine` service.

   ```bash
   systemctl restart ovirt-engine
   ```
Creating Event Notifications in the Administration Portal

Before creating event notifications, you must have access to an email server that can handle incoming automated messages and deliver these messages to a distribution list. You should also configure event notification services on the Engine. For more information, see Configuring Event Notification Services on the Engine.

To create event notifications in the Administration Portal:

1. Go to Administration and then click Users.
   
   The Users pane opens.

2. Under the User Name column, click the name of the user to display the detailed view for the user.

   A user does not appear in the Administration Portal until the user is created and assigned appropriate permissions. For more information, refer to Creating a New User Account.

3. Click the Event Notifier tab.

4. Click Manage Events.

   The Add Event Notification dialog box opens.

5. Enable and restart the ovirt-engine-notifier service to activate your changes.

   ```bash
   systemctl daemon-reload
   systemctl enable ovirt-engine-notifier.service
   systemctl restart ovirt-engine-notifier.service
   ```
5. Select the events for which you want to create notifications by selecting the check box next to individual events or event topic areas for notification.

The events available for notification are grouped under topic areas. By default, selecting the check box for a top-level topic area, such as General Host Events, selects all events under that topic area. You can optionally expand or collapse all the event topic areas by clicking Expand All or Collapse All. Additionally, you can click the arrow icon next to a specific top-level topic area to expand or collapse the events associated with a specific topic area.

6. For the Mail Recipient field, enter an email address.

7. Click OK to save the changes.

Canceling Event Notifications in the Administration Portal

To cancel event notifications in the Administration Portal:

1. Go to Administration and then click Users.

   The Users pane opens.

2. Under the User Name column, click the name of the user to display the detailed view for the user.

3. Click the Event Notifier tab.

4. Click Manage Events.

   The Add Event Notification dialog box opens.

5. Click Expand All, or the topic-specific expansion options, to display the events.

6. Clear the appropriate check boxes to cancel the notification for that event.

7. Click OK to save your changes.

Configuring the Engine to Send SNMP Traps

You can configure the Manager to send SNMP traps to one or more external SNMP managers. SNMP traps contain system event information that are used to monitor your virtualization environment. The number and type of traps sent to the SNMP manager can be defined within the Engine.

Before performing this task, you must have configured one or more external SNMP managers to receive traps, and know the following details:

- The IP addresses or fully qualified domain names of machines that act as SNMP managers. Optionally, determine the port through which the SNMP manager receives trap notifications; the default UDP port is 162.
- The SNMP community. Multiple SNMP managers can belong to a single community. Management systems and agents can communicate only if they are within the same community. The default community is public.
- The trap object identifier for alerts. The Engine provides a default OID of 1.3.6.1.4.1.2312.13.1.1. All trap types are sent, appended with event information, to the SNMP manager when this OID is defined.
To configure SNMP traps on the Engine:

1. Log in to the host that is running the Manager.

2. On the Engine, create the SNMP configuration file:

   ```shell
   # vi /etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf
   ```

   Default SNMP configuration values exist on the Engine in the events notifications configuration file (`ovirt-engine-notifier.conf`), which is available at the following directory path: `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf`. The values provided in this step are based on the default or example values provided in that file. To persist that your configuration settings persist across reboots, define an override file for your SNMP configuration (`20-snmp.conf`), rather than edit the `ovirt-engine-notifier.conf` file. For more information, see Configuring Event Notification Services on the Engine.

3. Specify the SNMP manager, the SNMP community, and the OID in the following format:

   ```
   SNMP_MANAGERS="manager1.example.com manager2.example.com:162"
   SNMP_COMMUNITY=public
   SNMP_OID=1.3.6.1.4.1.2312.13.1.1
   ```

   The following values can be configured in the `20-snmp.conf` file.

   ```
   #-------------------------#
   # SNMP_TRAP Notifications #
   #-------------------------#
   # Send v2c snmp notifications
   # Minimum SNMP configuration
   #
   # Create /etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf with:
   # SNMP_MANAGERS="host"
   # FILTER="include:*(snmp:) ${FILTER}"
   # Default whitespace separated IPv4/[IPv6]/DNS list with optional port, default is 162.
   # SNMP_MANAGERS="manager1.example.com manager2.example.com:164"
   # SNMP_MANAGERS=
   #
   # Default SNMP Community String.
   # SNMP_COMMUNITY=public
   #
   # SNMP Trap Object Identifier for outgoing notifications.
   # ( iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) redhat(2312) ovirt(13) engine(1) notifier)
   #
   # Note: changing the default will prevent generated traps from complying with OVIRT-MIB.txt.
   # SNMP_OID=1.3.6.1.4.1.2312.13.1.1
   #
   # Default SNMP Version. SNMP version 2 and version 3 traps are supported
   # 2 = SNMPv2
   ```
Configuring the Engine to Send SNMP Traps

```bash
# 3 = SNMPv3
SNMP_VERSION=3

# The engine id used for SNMPv3 traps
SNMP_ENGINE_ID=

# The user name used for SNMPv3 traps
SNMP_USERNAME=

# The SNMPv3 auth protocol. Supported values are MD5 and SHA.
SNMP_AUTH_PROTOCOL=

# The SNMPv3 auth passphrase, used when SNMP_SECURITY_LEVEL is set to AUTH_NOPRIV and AUTH_PRIV
SNMP_AUTH_PASSPHRASE=

# The SNMPv3 privacy protocol. Supported values are AES128, AES192 and AES256.
# Be aware that AES192 and AES256 are not defined in RFC3826, so please verify
# that your SNMP server supports those protocols before enabling them.
SNMP_PRIVACY_PROTOCOL=

# The SNMPv3 privacy passphrase, used when SNMP_SECURITY_LEVEL is set to AUTH_PRIV
SNMP_PRIVACY_PASSPHRASE=

# The SNMPv3 security level.
# 1 = NOAUTH_NOPRIV
# 2 = AUTH_NOPRIV
# 3 = AUTH_PRIV
SNMP_SECURITY_LEVEL=3

# SNMP profile support

# Multiple SNMP profiles are supported.
# Specify profile settings by using _profile suffix,
# for example, to define a profile to sent specific
# message to host3, specify:
# SNMP_MANAGERS_profile1=host3
# FILTER="include:VDC_START(snmp:profile1) ${FILTER}"
```

4. Define which events to send to the SNMP Manager.

By default, the following default filter is defined in the `ovirt-engine-notifier.conf` file; if you do not override this filter or apply overriding filters, no notifications are sent.

```bash
FILTER="exclude:\*"
```

The following are other common examples of event filters.

- Send all events to the default SNMP profile.

```bash
FILTER="include:\*(snmp:) ${FILTER}"
```

- Send all events with the severity `ERROR` or `ALERT` to the default SNMP profile:

```bash
FILTER="include:\*:ERROR(snmp:) ${FILTER}"
FILTER="include:\*:ALERT(snmp:) ${FILTER}"
```

5. Save the file.

6. Start the `ovirt-engine-notifier` service, and ensure that this service starts on boot.

```bash
# systemctl start ovirt-engine-notifier.service
# systemctl enable ovirt-engine-notifier.service
```
7. (Optional) Validate that traps are being sent to the SNMP Manager.
You can configure Oracle Linux Virtualization Manager so that your cluster is optimized and your hosts and virtual machine are highly available. You can also enable or disable devices (hot plug) while a virtual machine is running.

**Optimizing Clusters, Hosts and Virtual Machines**

Whether you have a new cluster, host, or virtual machine (VM) or existing ones, you can optimize resources such as CPU and memory and configure hosts and VMs for high availability.

**Configuring Memory and CPUs**

Using the Optimization tab when creating or editing a cluster, you can select the memory page sharing threshold for the cluster, and optionally enable CPU thread handling and memory ballooning on the hosts in the cluster. Some of the benefits are:

- VMs run on hosts up to the specified overcommit threshold. Higher values conserve memory at the expense of great CPU usage.
- Hosts to run virtual machines with a total number of CPU cores greater than the number of cores in the host.
- Memory overcommitment on VMs running on the hosts in the cluster.
- Memory Overcommitment Manager (MoM) runs Kernel Same-page Merging (KSM) when it can yield a memory saving benefit.

**Note**

If a VM is running Oracle products, such as Oracle Database or other Oracle applications, that require dedicated memory, configuring memory overcommitment is not an available option.

Using the Resource Allocation tab when creating or editing a VM, you can:

- set the maximum amount of processing capability a VM can access on its host.
- pin a virtual CPU to a specific physical CPU.
- guarantee an amount of memory for the VM.
- enable the memory balloon device for the VM. (Enable Memory Balloon Optimization must also be selected for the cluster.)
• improve the speed of disks that have a VirtIO interface by pinning them to a thread separate from the VM’s other functions.

Configuring Cluster Memory and CPUs

To optimize the usage of memory and CPUs at the cluster level:

1. Select the Optimization tab of the New Cluster or Edit Cluster window.

2. Choose a setting for Memory Optimization:
   - None - Disable memory overcommit
     Disables memory page sharing.
   - For Server Load - Allow scheduling of 150% of physical memory
     Sets memory page sharing threshold to 150% of the system memory on each host.
   - For Desktop Load - Allow scheduling of 200% of physical memory
     Sets memory page sharing threshold to 200% of the system memory on each host.

3. Under CPU Threads, check Count Threads As Cores to allow guests to use host threads as virtual CPU cores.

   Allowing hosts to run VMs with the total number of processing cores greater than the number of cores in the host may be useful for less CPU-intensive workloads.

4. Under Memory Balloon, check Enable Memory Balloon Optimization to enable memory overcommitment on VMs running on hosts in this cluster.

   The MoM starts ballooning where and when possible. It is only limited by the guaranteed memory size of every VM. Each VM in the cluster needs to have a balloon device with relevant drivers, which is included unless you specifically remove it. Every host in the cluster receives a balloon policy update when its Status changes to Up.

   **Note**
   Enable ballooning on VMs that have applications and loads that slowly consume memory, occasionally release memory, or stay dormant for long periods of time, such as virtual desktops.

5. Under KSM Control, check Enable KSM to enable MoM to run KSM when necessary and when it can yield a memory saving benefit that outweighs its CPU cost.

6. Click OK to save your changes.

Configuring Virtual Machine Memory and CPUs

To optimize the usage of memory and CPUs for a virtual machine:

1. Select the Resource Allocation tab of the New VM or Edit VM window.

2. Under CPU Allocation, for the CPU Shares drop-down list select the level of CPU resources a VM can demand relative to other VMs in the cluster.
   - Low=512
• **Medium** = 1024

• **High** = 2048

• **Custom** = Enter a number in the field next to the drop-down list

3. Under **Memory Allocation**, for **Physical Memory Guaranteed** enter an amount of memory.

   The amount of physical memory guaranteed for a VM should be any number between 0 and its defined memory.

4. Check **Memory Balloon Device Enabled** to enable the device for the VM and allow memory overcommitment.

   **Important**

   Since this check box is selected by default, make sure you have enabled memory ballooning for the cluster where the VM's host resides.

5. Under **I/O Threads**, check **I/O Threads Enabled** to improve the speed of disks that have a VirtIO interface by pinning them to a thread separate from the VM's other functions.

   This check box is selected by default.

6. Under **Queues**, check **Multi Queues Enabled** to create up to four queues per vNIC, depending on how many vCPUs are available.

   This check box is selected by default.

   To define a different number of queues per vNIC, you can create a custom property:

   ```
   # engine-config -s "CustomDeviceProperties={type=interface;prop={other-nic-properties;queues=[1-9][0-9]*}}"
   ```

   where **other-nic-properties** is a list of pre-existing NIC custom properties separated by semicolons.

7. Under **Queues**, check **VirtIO-SCSI Enabled** to enable or disable the use of VirtIO-SCSI on the VM.

   This check box is selected by default.

8. Click **OK** to save your changes.

### Configuring a Highly Available Host

Fencing keeps hosts in a cluster responsive. Fencing allows a cluster to react to unexpected host failures and enforce power saving, load balancing, and VM availability policies. You should configure the fencing parameters for your host's power management device and test their correctness from time to time.

A **Non Operational** host is different from a **Non Responsive** host. A **Non Operational** host can communicate with the Manager, but has incorrect configuration, for example a missing logical network. A **Non Responsive** host cannot communicate with the Manager.

In a fencing operation, a non-responsive host is rebooted, and if the host does not return to an active status within a prescribed time, it remains non-responsive pending manual intervention and troubleshooting.

The Manager can perform management operations after it reboots, by a proxy host, or manually in the **Administration Portal**. All the virtual machines running on the non-responsive host are stopped, and
highly available virtual machines are started on a different host. At least two hosts are required for power management operations.

**Important**
If a host runs virtual machines that are highly available, power management must be enabled and configured.

**Configuring Power Management and Fencing on a Host**

The Manager uses a proxy to send power management commands to a host power management device because the engine does not communicate directly with fence agents. The host agent (VDSM) executes power management device actions and another host in the environment is used as a fencing proxy. This means that you must have at least two hosts for power management operations.

When you configure a fencing proxy host, make sure the host is in:

- the same cluster as the host requiring fencing.
- the same data center as the host requiring fencing.
- **UP** or **Maintenance** status to remain viable.

Power management operations can be performed in three ways:

- by the Manager after it reboots
- by a proxy host
- manually in the Administration Portal

To configure power management and fencing on a host:

1. Click Compute and select Host.
2. Select a host and click Edit.
3. Click the Power Management tab.
4. Check Enable Power Management to enable the rest of the fields.
5. Check Kdump integration to prevent the host from fencing while performing a kernel crash dump. Kdump integration is enabled by default.

**Important**
If you enable or disable Kdump integration on an existing host, you must reinstall the host.

6. *(Optional)* Check Disable policy control of power management if you do not want your host's power management to be controlled by the scheduling policy of the host's cluster.
7. To configure a fence agent, click the plus sign (+) next to Add Fence Agent.

   The Edit fence agent pane opens.
8. Enter the Address (IP Address or FQDN) to access the host's power management device.
9. Enter the User Name and Password of the account used to access the power management device.
10. Select the power management device **Type** from the drop-down list.

11. Enter the **Port** (SSH) number used by the power management device to communicate with the host.

12. Enter the **Slot** number used to identify the blade of the power management device.

13. Enter the **Options** for the power management device. Use a comma-separated list of key-value pairs.
   - If you leave the **Options** field blank, you are able to use both IPv4 and IPv6 addresses
   - To use only IPv4 addresses, enter `inet4_only=1`
   - To use only IPv6 addresses, enter `inet6_only=1`

14. Check **Secure** to enable the power management device to connect securely to the host.
   
   You can use ssh, ssl, or any other authentication protocol your power management device supports.

15. Click **Test** to ensure the settings are correct and then click **OK**.
   
   **Test Succeeded, Host Status is: on** displays if successful.

   **Warning**

   Power management parameters (userid, password, options, etc.) are tested by the Manager only during setup and manually after that. If you choose to ignore alerts about incorrect parameters, or if the parameters are changed on the power management hardware without changing in the Manager as well, fencing is likely to fail when most needed.

16. Fence agents are sequential by default. To change the sequence in which the fence agents are used:
   
   a. Review your fence agent order in the **Agents by Sequential Order** field.
   
   b. To make two fence agents concurrent, next to one fence agent click the **Concurrent with** drop-down list and select the other fence agent.

   You can add additional fence agents to this concurrent fence agent group.

17. Expand the **Advanced Parameters** and use the up and down buttons to specify the order in which the Manager searches the host’s **cluster** and **dc** (data center) for a power management proxy.

18. To add a additional power management proxy:
   
   a. Click the plus sign (+) next to **Add Power Management Proxy**.

   The **Select fence proxy preference type to add** pane opens.
   
   b. Select a power management proxy from the drop-down list and then click **OK**.

   Your new proxy displays in the **Power Management Proxy Preference** list.

   **Note**

   By default, the Manager searches for a fencing proxy within the same cluster as the host. If the Manager cannot find a fencing proxy within the cluster, it searches the data center.

19. Click **OK**.
From the list of hosts, the exclamation mark next to the host’s name disappeared, signifying that you have successfully configured power management and fencing.

**Preventing Host Fencing During Boot**

After you configure power management and fencing, when you start the Manager it automatically attempts to fence non-responsive hosts that have power management enabled after the quiet time (5 minutes by default) has elapsed. You can opt to extend the quiet time to prevent, for example, a scenario where the Manager attempts to fence hosts while they boot up. This can happen after a data center outage because a host’s boot process is normally longer than the Manager boot process.

You can configure quiet time using the `engine-config` command option `DisableFenceAtStartupInSec`:

```bash
#engine-config -s DisableFenceAtStartupInSec=<number>
```

**Checking Fencing Parameters**

To automatically check the fencing parameters, you can configure the `PMHealthCheckEnabled` (false by default) and `PMHealthCheckIntervalInSec` (3600 sec by default) `engine-config` options.

```bash
#engine-config -s PMHealthCheckEnabled=True
#engine-config -s PMHealthCheckIntervalInSec=<number>
```

When set to true, `PMHealthCheckEnabled` checks all host agents at the interval specified by `PMHealthCheckIntervalInSec` and raises warnings if it detects issues.

**Configuring a Highly Available Virtual Machine**

If you have virtual machines that run critical workloads, you might consider configuring these VMs for high availability. Only a highly available virtual machine automatically restarts on its original host or live migrates to another host in the cluster if its original host:

- has a hardware failure and becomes non-operational.
- has scheduled downtime and is put in maintenance mode.
- loses communication with external storage and becomes unavailable.

If a virtual machine’s host is manually shut down, the VM does not automatically live migrate to another host.

**Note**

A highly available virtual machine does not restart if you shut it down cleanly from within the VM or the Manager or if you shut down a host without first putting it into maintenance mode.

To enable a VM to migrate to another available host in the cluster:

- Configure power management and fencing for the host running the highly available (HA) VM
- Ensure the HA VM’s host is part of a cluster of two or more available hosts
- Check that the destination host is operational
- Ensure the source and destination hosts can access the data domain where the virtual machine resides
Hot Plugging Devices on Virtual Machines

- Ensure the source and destination hosts can access the same virtual networks and VLANs.
- Check that the destination host has enough RAM and CPUs that are not in use to support the VM's requirements.

Virtual machines can also be restarted on another host even if the original host loses power if you have configured it to acquire a lease on a special volume on the storage domain. Acquiring a lease prevents the VM from being started on two different hosts, which could result in virtual machine disk corruption.

If you configure high availability:
- there is minimal service interruption because virtual machines are restarted within seconds and with no user intervention.
- your resources are balanced by restarting virtual machines on a host with low current resource utilization.
- you are ensured that there is sufficient capacity to restart virtual machines at all times.

You must configure high availability for each VM using the following steps:

1. Click **Compute** and then **Virtual Machines**.
2. In the list of VMs, click to highlight a VM and then click **Edit**.
3. In the **Edit Virtual Machine** window, click the **High Availability** tab.
4. Check **Highly Available** to enable HA for the VM.
5. From the **Target Storage Domain for VM Lease** drop-down list, select **No VM Lease** (default) to disable the functionality or select a storage domain to hold the VM lease.

Virtual machines are able to acquire a lease on a special volume on the storage domain. This enables a VM to start on another host even if the original host loses power. For more information, see **Storage Leases**.

6. From the **Resume Behavior** drop-down list, select **AUTO_RESUME**, **LEAVE_PAUSED**, OR **KILL**. If you defined a VM lease, KILL is the only option available.
7. From the **Priority** list, select **Low**, **Medium**, or **High**.

When VM migration is triggered, a queue is created in which the high priority VMs are migrated first. If a cluster is running low on resources, only the high priority VMs are migrated.

8. Click **OK**.

Hot Plugging Devices on Virtual Machines

You can enable or disable devices while a virtual machine is running.

**Hot Plugging vCPUs**

Hot plugging vCPUs means enabling or disabling devices while a VM is running.

**Note**

Hot unplugging a vCPU is only supported if the vCPU was previously hot plugged. A virtual machine’s vCPUs cannot be hot unplugged to less vCPUs than it was originally created with.
Before you can hot plug vCPUs, you must meet the following prerequisites:

- The VM's operating system must be explicitly set and must support CPU hot plug. For details, see https://www.ovirt.org/documentation/.
- Windows VMs must have the guest agents installed.

To hot plug a vCPU:

1. Click **Compute** and then select **Virtual Machines**.
2. Select a VM that is running and click **Edit**.
3. Click the **System** tab.
4. Change the value of **Virtual Sockets** as required.
5. Click **OK**.

### Hot Plugging Virtual Memory

Hot plugging memory means enabling or disabling devices while a VM is running. Each time you hot plug memory, it appears as a new memory device under **Vm Devices** on the VM's details page, up to a maximum of 16.

When you shut down and restart a VM, these devices are cleared from **Vm Devices** without reducing the VM's memory, allowing you to hot plug more memory devices.

**Note**

This feature is only available for the self-hosted engine Engine virtual machine, which is currently a technology preview feature.

To hot plug virtual memory:

1. Click **Compute** and then select **Virtual Machines**.
2. Select a VM that is running and click **Edit**.
3. Click the **System** tab.
4. Enter a new number for **Memory Size**. You can add memory in multiples of 256 MB. By default, the maximum memory allowed for the VM is set to 4x the memory size specified.
5. Click **OK**.
   - The **Pending Virtual Machine changes** window opens.
6. Click **OK** for the changes to take place immediately or check **Apply later** and then **OK** to wait for the next VM restart.
7. Click **OK**.
   - You can see the VM's updated memory in the **Defined Memory** field of the VM's details page and you can see the added memory under **Vm Devices**.

You can also hot unplug virtual memory, but consider:

- Only memory added with hot plugging can be hot unplugged.
• The VM's operating system must support memory hot unplugging.
• The VM must not have a memory balloon device enabled.

To hot unplug virtual memory:
1. Click **Compute** and then select **Virtual Machines**.
2. Click on the name of a VM that is running.
   The VM's details page opens.
3. Click **Vm Devices**.
4. In the **Hot Unplug** column, click **Hot Unplug** beside any memory device you want to remove.
   The **Memory Hot Unplug** window opens with a warning.
5. Click **OK**.

   Under **General** on the VM details page, the **Physical Memory Guaranteed** value for the virtual machine is decremented automatically.