



# Virtual Resources

---

- [Virtual Resources, page 1](#)
- [VDCs, page 2](#)
- [Application Containers, page 3](#)
- [VMs, page 10](#)
- [VM Action Requests, page 26](#)
- [Images, page 27](#)
- [Port Groups, page 29](#)
- [DV Port Groups, page 30](#)
- [Resource Pools, page 30](#)
- [Datastores, page 31](#)
- [Datastore Clusters, page 31](#)

## Virtual Resources

The **Virtual Resources** menu option displays a summary of your virtual resources with customizable reports. The Summary page displays an overview of all VDCs and VMs, reports for new VMs and deleted VMs, and trending reports for network usage, CPU usage, memory usage, disk usage.

You can manage the following virtual resources:

- VDCs
- Application Containers
- VMs
- VM Action Requests
- Images
- Port Groups
- DV Port Groups

- Resource Pools
- Datastores
- Datastore Clusters

## VDCs

During VM provisioning, you can associate a VM with a virtual data center (VDC). When you create a service request, you can choose the VDC on which the VM is provisioned. You can view a list of VDCs available for a group and choose the required VDC when provisioning the VM.

You can view available VDCs and their details by choosing **vDCs** under **Virtual Resources**.

The VDCs report displays all available VDCs, as well as the following information:

- Cloud
- vDC
- Type
- Lock State
- Total VMs
- Active VMs
- Custom Categories
- Status
- Tag

You can view additional details about a VDC by clicking on the row with the VDC and clicking **View Details**.

## Viewing VDC Details

The VDC details page displays related reports and trending data for the selected VDC. You can also view associated VMs, events, deleted VMs, and VM action requests.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VDCs**.
- Step 3** Click the row with the VDC that you want to view.
- Step 4** Click **View Details** to view the following information about the VDC:
- **Summary**—Displays trending reports for VDC CPU usage, VDC memory usage, VDC network usage, and VDC disk usage. Also displays reports for new and deleted VMs, and VM trending.
  - **VMs**—Displays all the VMs that belong to the VDC.
  - **Events**—Displays the current events associated with the VDC.

- Deleted VMs—Displays information about any VMs that have been deleted from the VDC. The information includes the cloud name, VM ID, VM label, instance name, host name, IP address, image ID, name, and time deleted.
- VM Action Requests—Displays all of the available action IDs and related information.

## Application Containers

Application containers are a templated approach to provisioning applications for end users. Each application container is a collection of VMware virtual machines (VMs) and/or bare metal servers (BMs) with an internal private network that is based on rules specified by the administrator. An application container can have one or more VMs and BMs and can be secured by a fencing gateway (for example, a Virtual Secure Gateway) to the external or public cloud.

Administrators can create one or more application container templates with the appropriate policies, workflows, and templates. The application container template determines how the application is provisioned for the end user.

You can view all available application containers and all associated VMs, bare metal servers, network tier mappings, L4-L7 services, and contracts. You can view additional details about an application container by clicking the row with the application container and clicking **View Details**.

## Permissions Required for Application Containers

The following table shows a list of the available application container actions and permissions required:

Task	End User Permissions
<a href="#">Viewing Application Container Details, on page 4</a>	Default
<a href="#">Viewing Application Container Reports, on page 5</a>	Default
<a href="#">Managing an Application Container's Power, on page 5</a>	Default
<a href="#">Decommissioning an Application Container, on page 6</a>	Default
<a href="#">Cloning an Application Container, on page 6</a>	Default
<a href="#">Adding a VM to an Application Container, on page 7</a>	Default
<a href="#">Adding a Bare Metal Server to a Deployed APIC Application Container, on page 7</a>	Default

Task	End User Permissions
<a href="#">Deleting an Application Container, on page 8</a>	Default
<a href="#">Accessing a VM Console, on page 8</a>	Default
<a href="#">Editing Resource Limits, on page 9</a>	Default
<a href="#">Editing a Cost Model, on page 9</a>	Default
<a href="#">Adding an Application Container Contract, on page 10</a>	Default

## Viewing Application Container Details

You can view VMs, bare metal servers, network tier mappings, and L4-L7 services that are associated with an application container. The End User Portal provides automatic configuration of the VNC console, and this option is displayed only if your administrator has configured the VNC console for the VM.

---

**Step 1** Choose **Virtual Resources**.

**Step 2** On the **Virtual Resources** page, click **Application Containers**.

**Step 3** Click the application container that you want to view.

**Step 4** Click **View Details** to view the following information about the application container:

- **Summary**—Displays information such as number of BMs and VMs per tier, custom label-tier name mapping, and resource limits for the container.
  - **Virtual Machines**—Displays the VMs provisioned for the application container, including details for each VM such as the VM name, VM type, status, IP address, guest OS, and the time the VM was provisioned.
  - **Bare Metal Servers**—Displays the bare metal servers provisioned as part of the application container, including details for each bare metal server such as the bare metal server name, OS type, and service request ID for each bare metal server.
  - **Tier Mapping**—Displays the tiers that correspond to the networks defined by your administrator and includes the VMs and BMs contained in each tier.
  - **L4 L7 Services**—Displays information about L4-L7 services, including the service request ID, service name, IP address, service type, device type, and consumer and provider tiers.
  - **Contracts**—Displays information about contracts created for the application container, including the source container, source network, destination container, and destination network.
-

## Viewing Application Container Reports

For each application container, you can generate summary reports, a detailed report with credentials, and a detailed report without credentials. If you choose to generate a report with credentials, the passwords appear in plain text. The report header displays the service request ID used to create the container.



---

**Note** Generating a report without credentials hides the passwords in the report.

---

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the row with application container for which you want to view reports.
  - Step 4** Click **View Reports**.
  - Step 5** On the **View Container Reports** screen, choose the type of report to generate from the **Select Report Type** drop-down list.
  - Step 6** Click **Submit**.
- 

## Managing an Application Container's Power

You can enable and disable power for an application container.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the application container that you want to power on or power off.
  - Step 4** Click **Power On Container** or **Power Off Container**.
  - Step 5** On the **Power On Container** or the **Power Off Container** screen, select the provisioned VMs to power on or power off.
  - Step 6** Click **Submit**.
-

## Decommissioning an Application Container

You can decommission an application container that you no longer require. When you decommission an application container, the provisioned VMs are powered off but not deleted.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the application container that you want to decommission.
  - Step 4** Click **Decommission Container**.
  - Step 5** On the **Decommission Container** screen, select the provisioned VMs to power off.
  - Step 6** Click **Submit**.
- 

## Cloning an Application Container

You can clone an existing application container. Cloning an application container retains all of the settings and configuration data with the VMs that are contained in the original application container.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the application container that you want to clone.
  - Step 4** Click **Clone Container**.
  - Step 5** On the **Clone Container** screen, specify the new container name and new container label. The container label must be unique.
  - Step 6** Click **Submit**.  
The cloned container appears in the Application Container table.
-

## Adding a VM to an Application Container

You can add a VM exclusively to any of the deployed application containers available for you or your group.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the application container to which you want to add one or more VMs.
  - Step 4** From the **More Actions** drop-down list, choose **Add VMs**.
  - Step 5** On the **Manage VMs** screen, choose a row and click the pencil icon.
  - Step 6** On the **Edit Virtual Machines Entry** screen, enter the number of additional VM instances to provision, and click **Submit**.
    - Note** Your administrator defines the maximum number of VM instances that you can provision. An error message appears if you enter a value higher than the maximum instances allowed.
  - Step 7** On the **Manage VMs** screen, click **Submit**.
- 

## Adding a Bare Metal Server to a Deployed APIC Application Container

Bare metal servers are supported only in APIC containers. You can add a bare metal server to a deployed APIC application container.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the application container to which you want to add one or more bare metal servers.
  - Step 4** From the **More Actions** drop-down list, choose **Add BMs**.
  - Step 5** On the **Add BMs** screen, click **Add** to add a new bare metal server.
  - Step 6** On the **Add Entry to Bare Metal Application Components** screen, complete the required fields.
  - Step 7** Click **Submit**.

The newly added bare metal server is added to the **Bare Metal Application Components** list.
  - Step 8** On the **Add BMs** screen, you can add more bare metal servers or click **Submit**.
-

## Deleting an Application Container

You can delete an application container that you no longer require. When you delete an application container, you also delete the resources that are provisioned for that application container. When the **Delete Container** action is initiated, the application container setup is rolled back, and a service request is created.

---

**Step 1** Choose **Virtual Resources**.

**Step 2** On the **Virtual Resources** page, click **Application Containers**.

**Step 3** Click the application container that you want to delete.

**Step 4** From the **More Actions** drop-down list, choose **Delete Container**.

**Step 5** On the **Delete Container** screen, click **Submit**.

**Note** If you choose to delete an application container with associated L4-L7 services, the L4-L7 services are also deleted.

---

## Accessing a VM Console

You can view the VM console of a VM associated with an application container.

### Before You Begin

VNC must be configured on the VM you want to access.

---

**Step 1** Choose **Virtual Resources**.

**Step 2** On the **Virtual Resources** page, click **Application Containers**.

**Step 3** Click the application container for which you want to view the VM console.

**Step 4** From the **More Actions** drop-down list, choose **Open Console**.

**Step 5** On the **Access VM Console** screen, choose a VM from the **Select VM** drop-down list.

**Step 6** Click **Submit**.

The console for the selected VM opens in a new browser window.

---



## Editing Resource Limits

You can edit the resource limits for an application container. You can specify the number of vCPUs, the amount of memory, the limit for maximum storage, and the maximum number of half-width and full-width servers for the container.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the application container for which you want to edit the resource limits.
  - Step 4** From the **More Actions** drop-down list, choose **Edit Resource Limits**.
  - Step 5** On the **Container Limits** screen, check **Configure Resource Limit**.
  - Step 6** Complete the required fields and click **Submit**.
- 

## Editing a Cost Model

A cost model is used to define the unit level costs of virtual resources such as CPU, RAM, and storage. These costs are used for chargeback calculations of VMs within the virtual infrastructure. Your administrator can map a cost model to an application container template. You can edit the cost model for an application container.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Application Containers**.
  - Step 3** Click the application container for which you want to edit the cost model.
  - Step 4** From the **More Actions** drop-down list, choose **Edit Cost Model**.
  - Step 5** On the **Container Cost Model** screen, choose a cost model from the **Cost Model** drop-down list. The drop-down list displays the available cost models mapped to the application container.
  - Step 6** Click **Submit**.
-

## Adding an Application Container Contract

Contracts are policies that enable inter-End Point Group (inter-EPG) communication. These policies are the rules that specify communication between application tiers.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **Application Containers**.
- Step 3** Click the application container to which you want to add a contract.
- Step 4** Click **View Details**.
- Step 5** On the detail page for the application container, click **Contracts**.
- Step 6** Click **Add Contract**.
- Step 7** On the **Add Contract** screen, complete the required fields, including the following:
- Choose the source network and destination network to which you want to apply the contract rule.  
If the contract is between the tiers of the same container, you can choose the tiers that belong to the same container, otherwise, you can choose the tiers from different containers.
  - Check **Create Rule** to create a filter rule.  
If **Create Rule** is not checked, only an empty contract is created.
  - Choose the protocol to use for communication.  
If you choose **TCP** or **UDP**, additional fields for the starting and ending range for the source port and destination port appear.
  - Check **Apply Both Directions** to apply the contract to the traffic from the source to the destination, and the traffic from the destination to the source.
  - From the **Action** drop-down list, choose the action to be taken for the traffic that matches the contract.
- Step 8** Click **Submit**.
- 

## VMs

You can perform post-provisioning lifecycle management actions that are permitted by your administrator. You can view the entire list of VMs provisioned using service requests under a user group. You can view the VMs report by choosing **VMs** under **Virtual Resources**.

The VMs report lists all available VMs, as well as the following information:

- Cloud
- VM-ID
- VM Label
- VM Name
- Host Name
- IP Address

- Image ID
- Power State
- VM Protected
- Group Name
- VDC
- Category
- Provisioned Time
- Scheduled Termination Time
- Last Status Update
- Guest OS Type
- VM Annotation
- Custom Attributes
- Assigned To User
- Users Can Access
- Users Can Manage
- Tags
- VMM Cloud

You can view additional details about a VM by clicking the row with the VM and clicking **View Details**.

**Note**

The VMs report no longer displays the vCenter VM ID and the vCenter IP fields in End User Portal versions 6.5 and later.

## Permissions Required for VMs

The following table shows a list of the available VM lifecycle management actions and permissions required:

Task	End User Permissions
<a href="#">Viewing VM Details, on page 13</a>	Default
<a href="#">Requesting Inventory Collection on a VM, on page 13</a>	Default
<a href="#">Launching the VM Client, on page 13</a>	Additional permissions required
<a href="#">Launching the VNC Console, on page 14</a>	Additional permissions required
<a href="#">Launching the VMRC HTML5 Console, on page 15</a>	Additional permissions required

<b>Task</b>	<b>End User Permissions</b>
<a href="#">Configuring the Lease Time for a VM, on page 15</a>	Additional permissions required
<a href="#">Managing a VM's Power, on page 16</a>	Additional permissions required
<a href="#">Creating a Snapshot, on page 17</a>	Additional permissions required
<a href="#">Reverting a Snapshot, on page 18</a>	Additional permissions required
<a href="#">Marking a Snapshot as Golden, on page 19</a>	Additional permissions required
<a href="#">Cloning a VM, on page 19</a>	Additional permissions required
<a href="#">Resizing a VM, on page 20</a>	Additional permissions required
<a href="#">Resynchronizing a VM, on page 21</a>	Additional permissions required
<a href="#">Creating a VM Disk, on page 21</a>	Additional permissions required
<a href="#">Adding a vNIC to a VM, on page 22</a>	Additional permissions required
<a href="#">Assigning a VM to a VDC, on page 22</a>	Additional permissions required
<a href="#">Moving a VM to a VDC, on page 23</a>	Additional permissions required
<a href="#">Cloning a VM as an Image, on page 24</a>	Additional permissions required
<a href="#">Converting a VM as an Image, on page 24</a>	Additional permissions required
<a href="#">Enabling and Disabling the VMRC Console on a VM, on page 25</a>	Additional permissions required
<a href="#">Mounting an ISO Image as a CD/DVD Drive, on page 25</a>	Additional permissions required
<a href="#">Unmounting an ISO Image as a CD/DVD Drive, on page 26</a>	Additional permissions required

## Viewing VM Details

The VM details page displays related reports and trending data for the selected VM. You can also view associated VM action requests, events, VM snapshots, and vNICs on the VMs details page.

---

**Step 1** Choose **Virtual Resources**.

**Step 2** On the **Virtual Resources** page, click **VMs**.

**Step 3** Click the row with the VM that you want to view.

**Step 4** Click **View Details** to view the following information about the VM:

- **Summary**—Displays trending reports for CPU usage, memory usage, network usage, and disk I/O. Also displays reports for overview, ownership, resources, storage, network, guest information, and catalog details.
  - **VM Action Requests**—Displays all of the available action IDs and related information.
  - **Events**—Displays the current events associated with the VM
  - **VM Snapshots**—Displays all of the available VM snapshots and related information.
  - **vNICs**—Displays all of the vNICs associated with the VM.
- 

## Requesting Inventory Collection on a VM

You can request on-demand inventory collection for a VM.

---

**Step 1** Choose **Virtual Resources**.

**Step 2** On the **Virtual Resources** page, click **VMs**.

**Step 3** Click the row with the VM for which you want to collect inventory.

**Step 4** From the **More Actions** drop-down list, choose **Inventory Collection Request for VM**.

**Step 5** On the **Request VM Inventory Collection** screen, click **Submit**.

The VMs report and the VM's detail page are refreshed with updated information from the inventory collection request.

---

## Launching the VM Client

You can access the VM client using web access or remote desktop.

**Note**

You can access a VM's login credential when it is set up for web access or remote desktop access. Your administrator must provide the proper catalog (and necessary privileges) from which the VM is provisioned.

**Before You Begin**

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM, for which you want to launch the VM client.
  - Step 4** Click **Launch VM Client**.
  - Step 5** On the **Launch Client** screen, choose an access scheme from the **Access Scheme** drop-down list.
  - Step 6** Click **Proceed**.
- 

## Launching the VNC Console

The VNC console provides access and full control capabilities for each VM. The VNC console is accessible using any standalone web browser, and a plug-in is not required. The End User Portal provides automatic configuration of the console, and this option is displayed only if your administrator has configured the VNC console for the VM.

**Before You Begin**

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Disable popup blockers in your browser.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM.
  - Step 4** On the **Launch VNC Console** screen, choose the keyboard mapping layout, and click **Submit**.
    - Tip** If the screen is blank, click in the black area and press **Enter**.
-

## Launching the VMRC HTML5 Console

The End User Portal enables you to launch an HTML5 based VMRC console that functions independently of web browser type and does not require a third-party plugin or additional clients.



---

**Note** The HTML5 VMRC SDK is supported with VMware vCenter version 6.0 or later.

---

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Prior to launching the VM from an HTML5 based VMRC console, you must access the VMware vSphere web client URL, such as `https://vCenterIP`, with your browser and accept the self-signed certificate. If you do not accept the self-signed certificate prior to launching the VMRC HTML5 console, an error appears stating that the console has been disconnected.



---

**Note** This is not applicable for VMware vCenters with trusted certificates.

---

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM.
  - Step 4** Click **VMRC Console (HTML5)**.  
The VM client is launched in a new browser window.
- 

## Configuring the Lease Time for a VM

You can configure a lease expiration time for a selected VM if your administrator has not configured a lease time using a standard catalog for VM provisioning. You can configure the lease time when creating a service request for a standard catalog, or after the VM has been provisioned. Once the lease time expires, the VM is shut down (powered off).

**Before You Begin**

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM, for which you want to configure the lease time.
- Step 4** Click **Configure Lease Time**.
- Step 5** On the **Configure Lease Time** screen, check **Set Lease Time** and set the date and time that you want the VM lease to expire.
- Note** You can only edit this field if your administrator has not specified a lease time in the catalog used for VM provisioning.
- Step 6** Click **Submit for Approval**.
- 

When the request is approved, the scheduled termination time is updated on the VMs report.

**Managing a VM's Power**

You can manage power settings for a VM using the following actions:

- Power On
- Power Off
- Suspend
- Shutdown Guest
- Standby
- Reset
- Reboot

**Before You Begin**

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM on which you want to execute the action.
- Step 4** Click one of the following actions, or choose the action from the **More Actions** drop-down list:
- **Power On**



- **Power Off**
- **Suspend**
- **Shutdown Guest**
- **Standby**
- **Reset**
- **Reboot**

**Step 5** On the **VM Task** screen, choose if you want to execute the action now or later. If you choose to execute the action later, choose the date and time for which you want to schedule the action. You can also provide comments for the action.

**Step 6** Click **Proceed**.

---

### **What to Do Next**

After you power on a VM, perform an inventory collection request to refresh the VM's IP address.

## **Snapshots**

A snapshot is a point-in-time image of the complete state of a VM. You can create and manage snapshots to use in the event of a recovery from a system disaster or malfunction. We recommend that you create snapshots periodically to preserve the current state of the VM. For example, you can create a snapshot of your VM in its stable form prior to performing a potentially risky system operation. After creating several snapshots, you can view the VM snapshot summary report to identify which snapshots you want to preserve for future use. These snapshots are referred to as "golden snapshots", and cannot be deleted.

### **Creating a Snapshot**

You can create a snapshot of the VM and all of its resources in their current state.

#### **Before You Begin**

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.



---

**Note** You must have VMware tools installed on the VM to use this option.

---

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM of which you want to create a snapshot.
- Step 4** From the **More Actions** drop-down list, choose **Create Snapshot**.
- Step 5** On the **Create Virtual Machine Snapshot** screen, enter a name and description for the snapshot.
- Step 6** Check **Snapshot Memory** if you want to include the VM memory in the snapshot.
- Step 7** Check **Quiesce Guest File System** to take the snapshot in Quiesce mode. Quiescing a file system brings the on-disk data of a physical or virtual computer into a state suitable for backups. This process may include operations such as flushing dirty memory buffers from the operating system's in-memory cache to disk, or other high-level application-specific tasks.
- Step 8** Click **Proceed**.
- 

## Reverting a Snapshot

You can revert to the most recent snapshot of the VM if the VM crashes or malfunctions for any reason. You can also select a specific snapshot to revert to, in case there is more than one snapshot available for the VM.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM that you want to revert to a snapshot.
- Step 4** From the **More Actions** drop-down list, choose **Revert Snapshot**.
- Step 5** On the **Revert Snapshot Task** screen, select the snapshot to which you want to revert and click **Proceed**.
- 

### What to Do Next

After you have reverted to a snapshot, the VM will be in the off state. You can power on your VM by clicking **Power ON**.

## Marking a Snapshot as Golden

After you create a snapshot of a provisioned VM, you can identify which snapshots you want to preserve for future use. You can mark a specific snapshot for a VM as a golden snapshot. This feature protects the snapshot from accidental deletion. The only way to delete a golden snapshot is to unmark the golden snapshot, and return its status to that of a standard snapshot.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM, for which you want to define a golden snapshot.
  - Step 4** From the **More Actions** drop-down list, choose **Mark Golden Snapshot**.
  - Step 5** On the **Mark Golden Snapshot Task** screen, select the snapshot that you want to mark as golden.
  - Step 6** Check **Mark As Golden Snapshot** to designate the snapshot as a golden snapshot.
  - Step 7** Click **Proceed**.
- 

## Cloning a VM

You can clone an existing VM to create an identical copy. Cloning can save you time by retaining the parameters that you want from the VM you are cloning while allowing you to make adjustments needed for the new VM. The new name given to the cloned VM is defined in the system policy.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM that you want to clone.
  - Step 4** From the **More Actions** drop-down list, choose **Clone**.
  - Step 5** On the **Select Groups** screen, check **Assign to User** to assign the VM to a user.
  - Step 6** Check **Use Linked Clone** to clone a VM from a linked clone, then complete the required fields and click **Next**.  
A linked clone is a copy of a VM that shares virtual disks with the parent VM. A linked clone is made from a snapshot of the parent VM and must have access to the parent VM. Without access to the parent VM, a linked clone is disabled.
  - Step 7** On the **Customization Options** screen, complete the fields including the following:
    - a) Choose to allow or disallow users to retrieve VM access credentials from the **Credential Options** drop-down list.

You can choose the **Do not share** option if you want to send the credentials privately to another user.

- b) Check **Enable** under **Post Provisioning Custom Actions** if you want to attach a workflow. You can choose a workflow to start when provisioning starts from the **Workflow** drop-down list.

- Step 8** Click **Next**.
- Step 9** On the **Deployment Configuration** screen, complete the required fields and then click **Next**.
- Step 10** On the **Custom Specifications** screen, complete the required fields and then click **Next**.
- Step 11** On the **Custom Workflow** screen, complete the required fields if the specified workflow requires user inputs and then click **Next**.
- Step 12** In the **Select Datastores** screen, if applicable, choose the datastores to assign to the VM disks and then click **Next**.
- Step 13** On the **Select VM Networks** screen, if applicable, choose the VM network and select one or more clouds that you want associated with the VM and then click **Next**.
- Step 14** On the **Summary** screen, review the information for accuracy.
- Step 15** Click **Submit**.
- 

## Resizing a VM

You can resize an existing VM by specifying new values for the CPU count and the memory. The new values for the CPU cost and memory cost are calculated based on the new values that you specify for the VM.



**Note** If CPU Hot Add and Memory Hot Add are not enabled for the VM, suspend or power off the VM before resizing the VM.

---

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

---

- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM that you want to resize.
- Step 4** Click **Resize VM**.
- Step 5** On the **Resize VM** screen, choose new values for the CPU count and memory from the **New CPU Count** and **New Memory** drop-down lists.  
The **New CPU Cost** and **New Memory Cost** fields recalculate based on the values you have chosen.
- Step 6** Click **Resize**.
-

## Resynchronizing a VM

You can set the interval of time to have a VM resynchronize its time periodically. If you set the time interval to zero minutes, the End User Portal immediately resynchronizes the VM.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM that you want to resynchronize.
  - Step 4** From the **More Actions** drop-down list, choose **VM Resync**.
  - Step 5** On the **Resync VM** screen, choose a time interval in minutes from the **Max Wait Time** drop-down list. Values range from zero to 30.
  - Step 6** Click **Submit**.
- 

## Creating a VM Disk

You can add an additional disk with a custom size to provisioned or discovered VMs.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM to which you want to add a VM disk.
  - Step 4** From the **More Actions** drop-down list, choose **Create VM Disk**.
  - Step 5** On the **Create VM Disk** screen, specify the new disk size in GB and select the disk type from the **Select Disk Type** drop-down list.
  - Step 6** Select a datastore from the **Select Datastore** drop-down list.  
The datastore's availability depends on the storage policy that is associated with the VM (specifically the VM's VDC).
  - Step 7** Check **Thin Provision** to use thin provisioning during VM creation.  
Thin provisioning enables dynamic allocation of the physical storage capacity to increase VM storage utilization.
  - Step 8** Check **Compute New Disk Cost** to calculate and display the disk cost, per hour.

The new disk cost is based on the new disk size and the datastore you specify for the VM disk.

**Step 9** Click **Create**.

---

## Adding a vNIC to a VM

You can add multiple vNICs to a VM. You have the option of either adding or replacing a vNIC in a VM. The options available depend on the network policy mapped to your VDC and associated to the particular VM.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

---

**Step 1** Choose **Virtual Resources**.

**Step 2** On the **Virtual Resources** page, click **VMs**.

**Step 3** Click the row with the VM to which you want to add a vNIC.

**Step 4** From the **More Actions** drop-down list, choose **Add vNICs**.

**Step 5** On the **Add vNIC to Container Network** screen, choose the network to which you want to add the vNIC.

**Step 6** Enter the required VM credentials.

**Step 7** Click **Submit**.

**Note** The VM is powered off to add the vNIC. The VM is powered on once the action is completed.

---

## Assigning a VM to a VDC

You can assign a VM to a group or VDC without making any modifications to the VM.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

---

**Step 1** Choose **Virtual Resources**.

**Step 2** On the **Virtual Resources** page, click **VMs**.

**Step 3** Click the row with the VM that you want to assign to a VDC.

**Step 4** From the **More Actions** drop-down list, choose **Assign VMs to VDC**.

**Step 5** On the **Assign VMs to VDC** screen, click **Assign**.

---

## Moving a VM to a VDC

You can move a VM to a VDC so that the rules of the VDC system policy persist in the VM. The VM that is moved to the VDC replaces the existing VM. When moving a VM to a VDC, you can also make modifications to the VM.



---

**Note** The old VM is deleted. The new VM name is assigned according to the system policy.

---

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM that you want to move to a VDC.
- Step 4** From the **More Actions** drop-down list, choose **Move VM to VDC**.
- Step 5** On the **Select Groups** screen, check **Assign to User** to assign the VM to a user.
- Step 6** If applicable, check **Use Linked Clone** to clone a VM from a linked clone, complete the required fields, and then click **Next**.  
A linked clone is a copy of a VM that shares virtual disks with the parent VM. A linked clone is made from a snapshot of the parent VM and must have access to the parent VM. Without access to the parent VM, a linked clone is disabled.
- Step 7** On the **Customization Options** screen, if modifications are required, complete the fields including the following:
- Choose to allow or disallow users to retrieve VM access credentials from the **Credential Options** drop-down list. You can choose the **Do not share** option if you want to send the credentials privately to another user.
  - Check **Enable** under **Post Provisioning Custom Actions** if you want to attach a workflow. From the **Workflow** drop-down list, you can choose a workflow to start when provisioning starts.
- Step 8** Click **Next**.
- Step 9** On the **Deployment Configuration** screen, update the required fields as necessary and then click **Next**.
- Step 10** On the **Custom Specifications** screen, update the required fields as necessary and then click **Next**.
- Step 11** On the **Custom Workflow** screen, complete the required fields if the specified workflow requires user inputs and then click **Next**.
- Step 12** On the **Select Datastores** screen, if applicable, choose the datastores to assign to the VM disks and then click **Next**.
- Step 13** On the **Select VM Networks** screen, if applicable, choose the VM network, select one or more clouds that you want associated with the VM, and then click **Next**.
- Step 14** On the **Summary** screen, review the information for accuracy.
- Step 15** Click **Submit**.
-

## Cloning a VM as an Image

You can clone a VM and save the VM image as a template for future provisioning.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM that you want to clone as an image.
  - Step 4** From the **More Actions** drop-down list, choose **Clone VM as Image**.
  - Step 5** On the **Clone VM as Image** screen, enter the name for the new image template.
  - Step 6** Click **Submit**.  
The new image appears on the Images page.
- 

### What to Do Next

You can provision a VM using the image. See [Converting an Image to a VM, on page 28](#).

## Converting a VM as an Image

You can convert an existing VM into an image that you can use for VM provisioning. You can convert a VM into an image if you no longer require the VM but want to retain the image for future provisioning. When you convert an existing VM into an image, the VM is taken offline and deleted.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM that you want to convert into an image.
  - Step 4** From the **More Actions** drop-down list, choose **Convert VM as Image**.
  - Step 5** On the **Convert VM as Image** screen, click **Submit**.  
The new image appears on the Images page.
- 

### What to Do Next

You can provision a VM using the image. See [Converting an Image to a VM, on page 28](#).



## Enabling and Disabling the VMRC Console on a VM

VMware vSphere contains the VMRC browser plug-in that can be loaded in supported web browsers. Web applications running in the browser can use the VMRC browser plug-in to access virtual machine console functions by using the VMRC JavaScript API. With a web application that uses the VMRC browser plug-in and the VMRC API, you can remotely access, and interact with, a virtual machine from any system that has the appropriate web browser and operating system.

By default, the VMRC console is disabled for all the discovered VMs. You can enable and disable the VMRC console on a VM.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **VMs**.
  - Step 3** Click the row with the VM on which you want to enable or disable the VMRC console.
  - Step 4** From the **More Actions** drop-down list, choose **Enable/Disable VMRC Console**.
  - Step 5** On the **Enable VMRC Console Access** screen, check **Enable VMRC Console**.  
Alternately, you can uncheck the box to disable VMRC console access if it is already enabled on the VM.
  - Step 6** Click **Submit**.
- 

### What to Do Next

Once you have enabled VMRC console access, you can launch the VM client from VMRC. See [Launching the VM Client](#), on page 13.

## Mounting an ISO Image as a CD/DVD Drive

An ISO is a disk image. You can mount ISO images on the VM without using a physical drive. Once mounted in your virtual machine, you can open, extract, and use the files from a virtual CD/DVD drive without a physical disk.

**Before You Begin**

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM on which you want to mount an ISO image.
- Step 4** From the **More Actions** drop-down list, choose **Mount ISO Image As CD/DVD Drive**.
- Step 5** On the **CD/DVD Drive Mount ISO** screen, choose the ISO image from the list of available images.
- Step 6** Choose one of the following options:
- **Create New CD/DVD Drive** and check **Power OFF VM**.
  - **Use Existing CD/DVD Drive** and choose the drive from the **Select DVD/DVD Drive** drop-down list.
- Step 7** Click **Submit**.  
The new or existing CD/DVD drive is mapped to your VM. You can log into the VM to view the mapped drive.
- 

## Unmounting an ISO Image as a CD/DVD Drive

You can unmount an ISO image already attached to CD/DVD drive on the virtual machine.

**Before You Begin**

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
- Step 2** On the **Virtual Resources** page, click **VMs**.
- Step 3** Click the row with the VM on which you want to unmount an ISO image.
- Step 4** From the **More Actions** drop-down list, choose **UnMount ISO Image As CD/DVD Drive**.
- Step 5** On the **CD/DVD Drive UnMount ISO** screen, choose the CD/DVD drive to unmount from the **Select CD/DVD Drive** drop-down list.
- Step 6** Click **Submit**.
- 

## VM Action Requests

You can view all available VM action requests and their details by choosing **VM Action Requests** under **Virtual Resources**.

You can also view VM action requests associated with a specific VM by choosing **VM Action Requests** on the VM's details page.

The VM Action Requests report displays all available VM action requests, as well as the following information:

- VM ID
- Action ID
- User Name
- Comment
- Schedule Time
- Status

## Images

An image is a template that can be used to create and provision virtual machines (VMs). An image typically includes a specified operating system and a configuration that provides virtual counterparts to hardware components. Images offer a secure way of preserving a VM's configuration that you want to deploy multiple times.

You can view all available VM images and their details by choosing **Images** under **Virtual Resources**. The image IDs in the Images report have been assigned to you or your group. You can use an image ID to provision a new VM. Additionally you can select and delete any image IDs that you do not require.

The Images report displays all available images, as well as the following information:

- ID
- Cloud
- Image ID
- Parent Node
- Datacenter
- Guest OS
- VMware Tools Installed
- VMware Tools Version
- VM Version
- Platform
- Architecture
- Number of CPUs
- Memory (MB)
- Provisioned Disk (GB)
- Image Location
- CPU Reservation (MHz)

- CPU Limit (MHz)
- CPU Shares
- Memory Reservation (MHz)
- Memory Limit (MHz)
- Memory Shares
- Uncommitted Storage (GB)
- Group/User

## Permissions Required for Images

The following table shows a list of the available image actions and permissions required:

Task	End User Permissions
<a href="#">Converting an Image to a VM, on page 28</a>	Additional Permissions Required
<a href="#">Deploying a VM from a Template, on page 29</a>	Additional Permissions Required

## Converting an Image to a VM

You can use an image ID that is assigned to you or your group to provision a new VM. When you convert an image to a VM, a service request is created.

You can view the associated service request by choosing **Services**, selecting the **Service Request ID**, and clicking **View Details**.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Images**.
  - Step 3** Click the row with the image that you want to convert to a VM.
  - Step 4** Click **Convert as VM**.
  - Step 5** On the **Convert Image as VM** screen, check **Assign VM** to select the user group to which you want to assign the VM. If unchecked, the VM will be assigned to the default group and default VDC.
  - Step 6** Complete the fields, including the VDC and category, and click **Submit**.
-

## Deploying a VM from a Template

You can deploy a VM from a template in the image report that is provided by your administrator.

### Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

- 
- Step 1** Choose **Virtual Resources**.
  - Step 2** On the **Virtual Resources** page, click **Images**.
  - Step 3** Click the row with the image that from which you want to deploy a VM.
  - Step 4** Click **Deploy VM from the Template**.
  - Step 5** On the **Deploy VM from the Template** screen, click **Assign To User** to assign the VM to a user.
  - Step 6** Check **Use Linked Clone** to clone a VM from a linked clone, and choose the snapshot to associate with the linked clone.
  - Step 7** Click **Next**.
  - Step 8** On the **Customizations Option** screen, specify the option to be customized for the provisioned VM and click **Next**.
  - Step 9** On the **Deployment Configuration** screen, complete the fields to choose where to deploy the VM, to choose to perform provisioning now or later, and to determine how long to keep the deployed VMs running.
  - Step 10** Click **Next**.
  - Step 11** On the **Custom Specification** screen, complete the fields for custom CPU and memory parameters, if applicable.
  - Step 12** Click **Next**.
  - Step 13** On the **Select Datastores** screen, choose the VM disk to which you want to assign the datastores.
  - Step 14** Click **Next**.
  - Step 15** On the **Select VM Networks** screen, choose the VM network.
  - Step 16** Click **Next**.
  - Step 17** On the **Summary** screen, review the information and click **Submit**.
- 

## Port Groups

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

You can view all available port groups and their details by choosing **Port Groups** under **Virtual Resources**.

The Port Groups report displays all available port groups and the following information:

- Host Node
- vSwitch Name
- Port Group Name
- Port Group Type

- VLAN ID
- Group/User

## DV Port Groups

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

A distributed virtual (DV) port group is a port group associated with a distributed switch. It specifies port configuration options for each member port. A DV port group defines how a connection is made through the switch to the network. You can view all available DV port groups and their details by choosing **DV Port Groups** under **Virtual Resources**.

The DV Port Groups report displays all available DV port groups and the following information:

- Host Node
- vSwitch Name
- Port Group Name
- Port Group Type
- VLAN ID
- Promiscuous Mode (Accept)
- Group/User

## Resource Pools

You can view available clouds and related configuration information. The resource details are at the host node level. You can view the Resource Pools report by choosing **Resource Pools** under **Virtual Resources**.

The Resource Pools report displays all available resource pools, as well as the following information:

- ID
- Cloud
- Datacenter Name
- Owner
- Resource Pool Name
- Parent
- Status
- CPU Configured Reservation (MHz)
- CPU Limit (MHz)
- CPU Used Reservation (MHz)
- CPU Expandable Reservation

- Memory Configured Reservation
- Memory Limit (MHz)
- Memory Used Reservation (MHz)
- Memory Expandable Reservation
- Group/User
- Tag

## Datastores

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

A datastore is the storage repository for virtual machines and their data. A datastore can be either a Network File System (NFS) or Virtual Machine File System (VMFS). Administrators can use the task library to create datastores from physical storage. Newly created and existing datastores are then used in VDC storage policies to provide a policy-based framework, from which you can select an appropriate datastore during VM provisioning. Datastores can also be identified as ISO image repositories to aid in ISO-based VM provisioning.

You can view available datastores and their details by choosing **Datastores** under **Virtual Resources**.

The Datastores report displays all available datastores and the following information:

- Cloud
- Data Store Name
- Data Center Name
- Capacity (GB)
- Free (GB)
- Free (%)
- Used (GB)
- Is Accessible
- Number of VMs
- Number of Hosts
- Extended Type
- Display Name
- Group/User

## Datastore Clusters

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

A datastore cluster is a collection of datastores with shared resources and a shared management interface. You can view available datastore clusters and their details by choosing **Datastore Clusters** under **Virtual Resources**.

The Datastore Clusters report displays all available datastore clusters and the following information:

- ID
- Cloud
- Data Center Name
- Datastore Cluster Name
- Capacity (GB)
- Free Space (GB)
- I/O Metrics
- Group/User
- Storage DRS
- Automation Level
- Utilized Space Threshold (%)
- I/O Latency
- Type
- Tag