

VI3 Roles and Permissions

VMware Infrastructure has a rich set of privileges for designating what actions may be performed on which objects. The design and concepts behind this are explained in the paper [Management VirtualCenter Roles and Permissions](#). That paper gives some specific use case examples, and this document aims to extend that list and provide more practical examples of how to configure roles and permissions to grant the capabilities you wish without enabling too much.

Concepts

The above-referenced document goes over the concepts in VI Roles and Permissions in more detail. Here we present an overview of the most important ones.

Definitions

Privilege: the right to perform a specific action, e.g. power on a VM, change a configuration value, or create a task

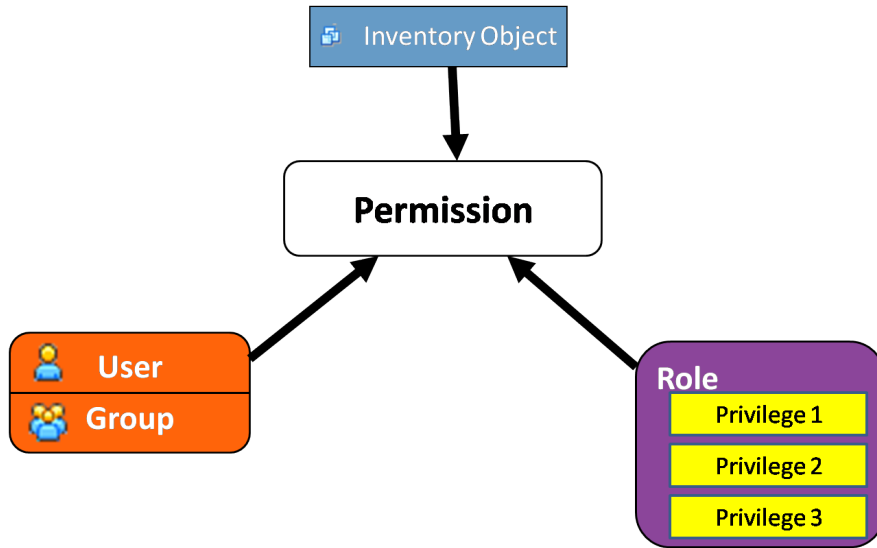
Role: a collection of privileges

Object: the entity on which roles are applied, e.g. VM, host, folder, cluster, etc.

User/Group: the individual or set of individuals to which privileges or roles are granted

Permissions: the application of a role to a user/group for an object.

The following diagram illustrates these concepts (click to enlarge):



Datstores and Networks have no direct privileges

In VI3, Datstores and Networks have no privileges directly defined for them. Instead, they inherit privileges from their parent datacenter, for example, "Read-Only". As a result, there is no way to assign a role for just one datastore or network in a datacenter -- the role applies to all or nothing. This has a few important implications:

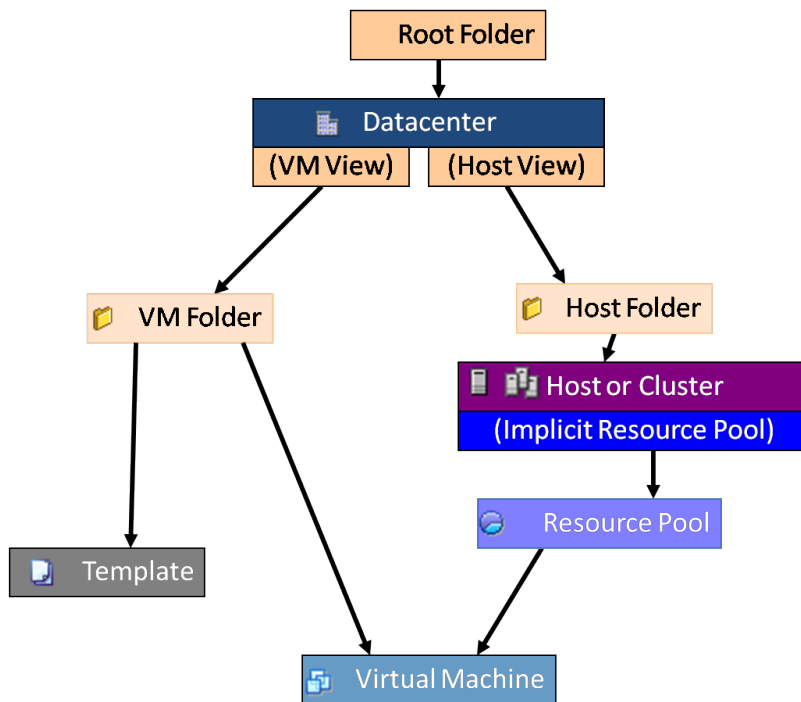
- If you want to allow users to create VMs, they will have the ability to create them on *all* datstores in the datacenter. They will also be able to assign the VM to *any* virtual network in the datacenter
- You cannot grant the ability to browse a datastore for ISO images, for example, without being able to see all files on the datastore

One way to limit what network a user can utilize is to only allow the user to deploy from a VM template. Within the template, you specify exactly which network the new VMs should use, and the user cannot modify this (unless they are granted the modify privilege). You would need to create a unique template for each network that the user should be allowed to use. Note that this method cannot be used to restrict datastore access. Datastore access can only be limited via the parent "datacenter" object, e.g. by not allowing users to deploy within "datacenters" that contain sensitive datstores.

VMs inherit privileges from two sources

VMs appear in the inventory in two places: under the "Virtual Machines and Templates" view and the "Hosts and Clusters" view. This is also reflected in their privilege inheritance: VMs inherit privileges from both the containing host/cluster object as well as the containing VM/Template folder. Under Hosts and Clusters, possible containing objects include: folders, clusters, hosts, and resource pools. The two views and hierarchies become unified at the

top level datacenter (or any folder that contains the datacenter). This is illustrated in the following diagram (click to enlarge):



Certain tasks require privileges on both sides of the hierarchy. For example, to create a VM, you need to have the "VM > Inventory > Create" privilege on a VM folder (in the VM view) as well as "Resource > Assign VM to Resource Pool" somewhere on an object in the Host view (folder, cluster, host, or resource pool). If you have a role which contains both these privileges, and you assign it at the datacenter level, it will propagate down both sides of the hierarchy. If, however, you want to limit its scope, then you'd need to apply it separately to individual subsections on each side of the hierarchy.

One way to keep this all straight is to create roles that are relevant only to one side of the hierarchy, and then apply these roles explicitly to the users or groups.

Clusters and Hosts implicitly are resource pool

Some tasks require privileges assign to a resource pool. For example, to create a VM, one of the privileges needed is "Assign VM to Resource Pool". What might not be obvious is that both clusters and hosts implicitly are resource pools. So, if there is no explicit resource pool defined below a cluster or a host, then you need to assign this privilege to that cluster or host.

Privileges Needed to Create a Virtual Machine

<i>Privilege</i>	<i>Object</i>
Virtual Machine > Inventory > Create	A destination folder of virtual machines in the datacenter, a folder containing a datacenter, or the datacenter itself if you do not use folder-based organization.
Virtual Machine > Configuration > Add New Disk OR, Only if including a virtual disk device that refers to an existing virtual disk file (not RDM). Virtual Machine > Configuration > Add Existing Disk Note: One of these two is required	A destination folder of virtual machines in the datacenter; a folder containing a datacenter, or the datacenter itself if you do not use folder-based organization.
Only if including a raw device mapping (RDM) or SCSI pass-through device for use by the virtual machine. Virtual Machine > Configuration > Raw Device	A destination folder of virtual machines in the datacenter; a folder containing a datacenter, or the datacenter itself if you do not use folder-based organization.
Resource > Assign VM to Resource Pool	A destination resource pool, host, or cluster.
Read-Only role	The datacenter that contains the datastore on which the virtual machine will reside or a folder containing the datacenter. Propagation does not have to be enabled for the datacenter, but it must be enabled for a folder.

Privileges Needed for various Inventory Manipulations

<i>Task</i>	<i>Required Privileges</i>
Migrate a virtual machine	On the virtual machine, you need Resource > Migrate if the virtual machine is powered on or Resource > Relocate if the virtual

	<p>machine is powered off. Also requires Resource > Assign Virtual Machine to Resource Pool if destination is a different resource pool from the source.</p>
<p>Move a host into a folder</p>	<p>Host > Inventory > Modify Cluster on the source cluster, Host > Inventory > Move Host on the host, and Host > Inventory > Add Standalone Host on the target Folder.</p>
<p>Move a virtual machine, standalone host, folder, cluster or datacenter into a folder</p>	<p>Folder > Move if the object is a folder, Datacenter > Move if the object is a datacenter, Host > Inventory > Move Cluster/Standalone Host if the object is a cluster or standalone host, Virtual Machine > Inventory > Move if the object is a virtual machine or virtual machine template. These privileges are checked against the source, destination, and object being moved.</p>
<p>Move a set of resource pools or virtual machines into a resource pool</p>	<p>If the object being moved is a resource pool, Resource > Move Pool must be held on the pool being moved, its former parent pool, and the target pool. If the object is a virtual machine, Resource > Assign Virtual Machine to Resource Pool must be held on the target pool and the virtual machine.</p>
<p>Remove all child resource pools</p>	<p>The Resource > Remove Pool privilege must be held on the parent and each of its immediate children to be removed. The Resource > Assign Virtual Machine to Resource Pool privilege must be held on the parent resource pool as well as on the virtual machine.</p>