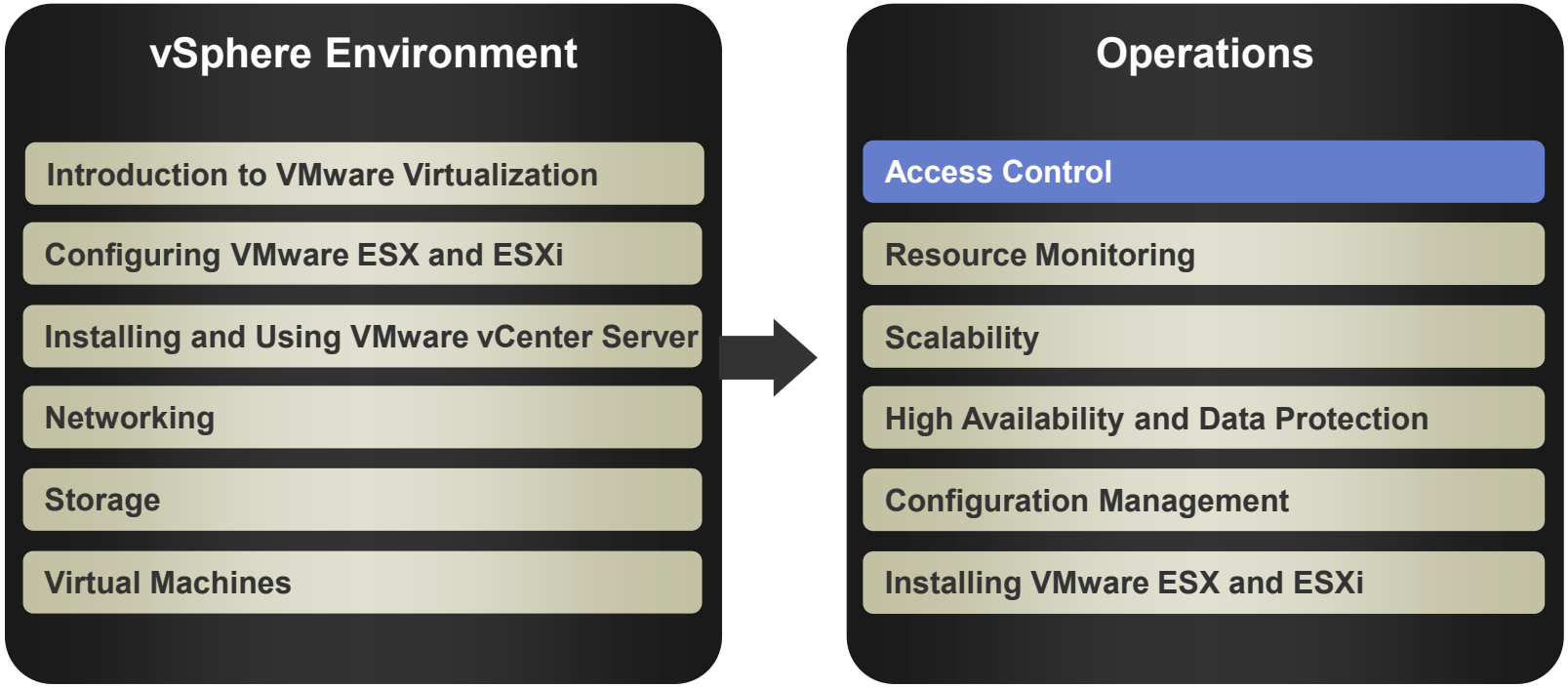
Access Control

Module 8

You Are Here



Importance

- When there are multiple users accessing the VMware® vSphere™ environment, it is a best practice to give each of your users only the necessary permissions and nothing more. VMware vCenter™ Server allows flexible assignment of permissions.

Lesson Objectives

- Define a permission
- Describe the rules for applying permissions
- Create a custom role
- Create a permission
- Describe the benefits of using VMware vSphere Web Access
- List tasks you can perform in vSphere Web Access

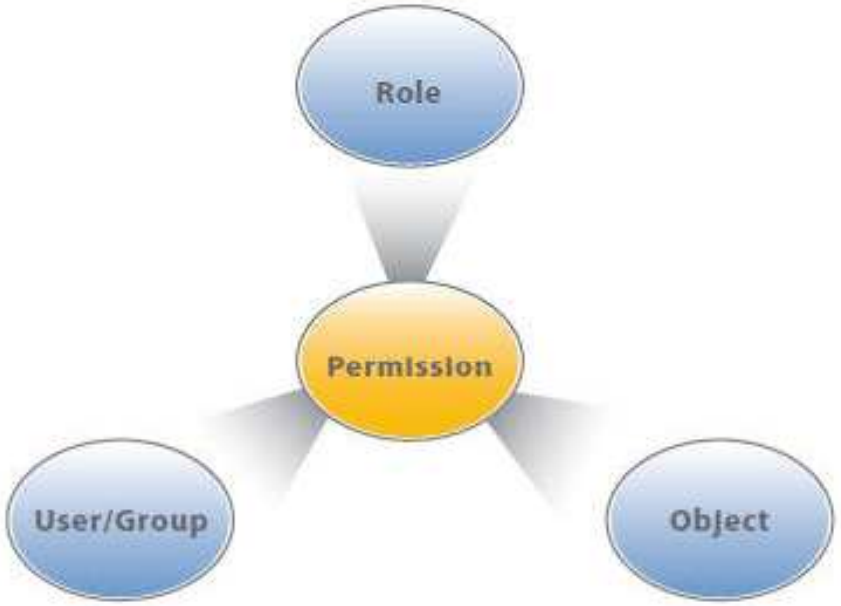
Access Control Overview

The access control system allows the vCenter Server administrator to specify which users or groups can perform which actions on which objects.

Key concepts:

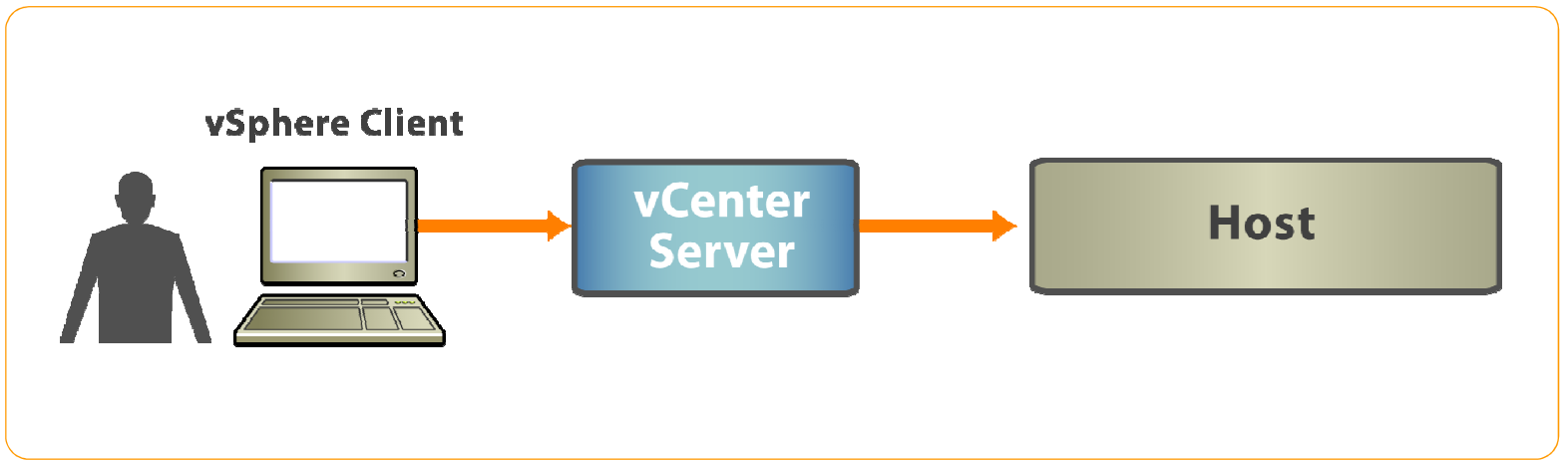
- Privilege – Defines an action that can be performed
- Role – A set of privileges
- Object – The target of the action
- Windows user/group – Indicates who can perform the action

Together, a role, a user/group, and an object define a permission.



Users and Groups

vCenter Server users and groups are those defined in the vCenter Server's Windows domain.

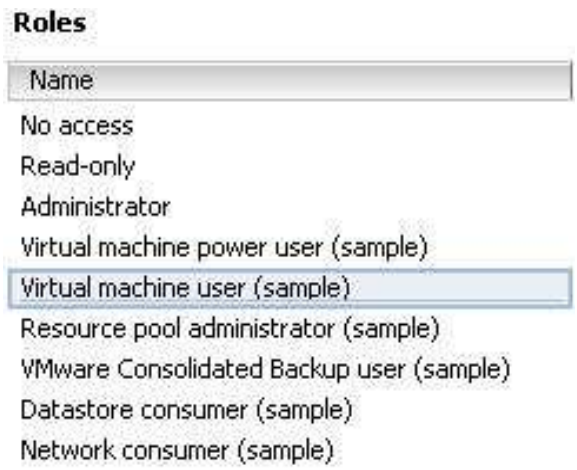


Roles and Privileges

Roles are collections of privileges.

- They allow users to perform tasks.
- They are grouped in categories.

There are system roles, sample roles, and custom-built roles.



Objects

Objects are entities upon which actions are performed.

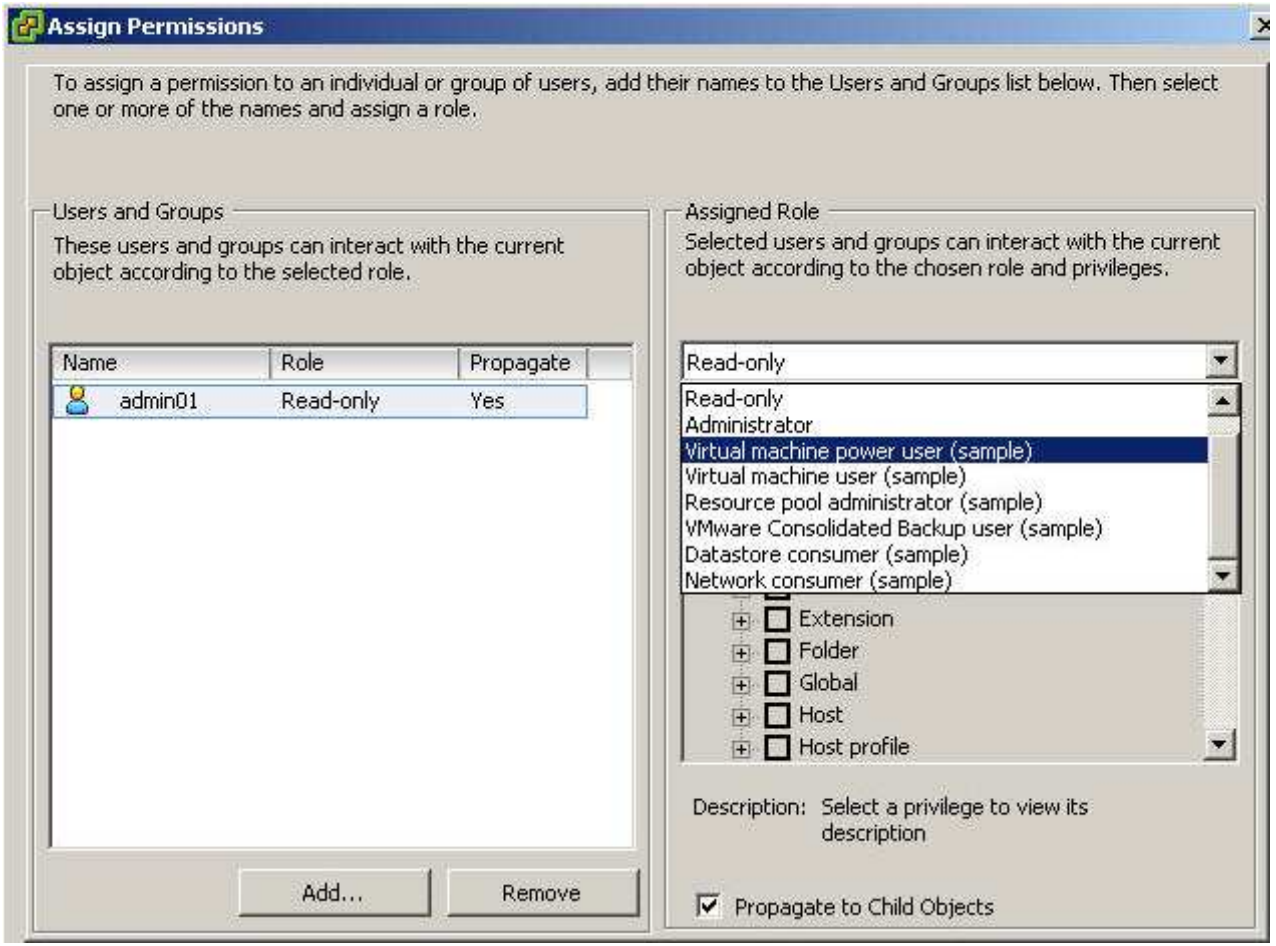
- Examples of objects are datacenters, folders, resource pools, clusters, hosts, datastores, networks, and virtual machines.

All objects have a Permissions **tab.**

- This tab shows what user/group and role are associated with the selected object.

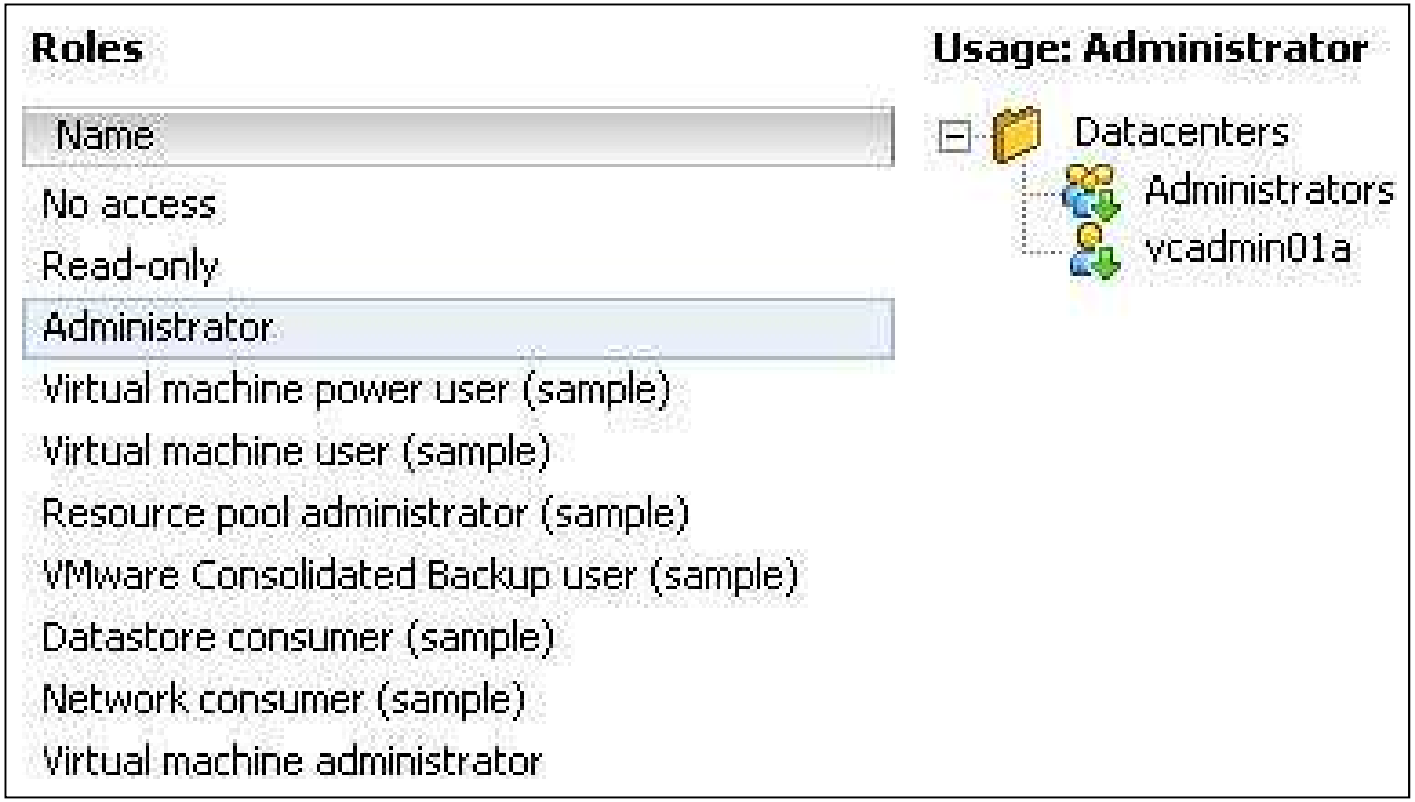
Assigning Permissions

- To add a permission, go to the object's **Permissions** tab, right-click the viewing area, then select **Add Permission**.
- Select a user and a role.
- You can also propagate the permission to child objects.



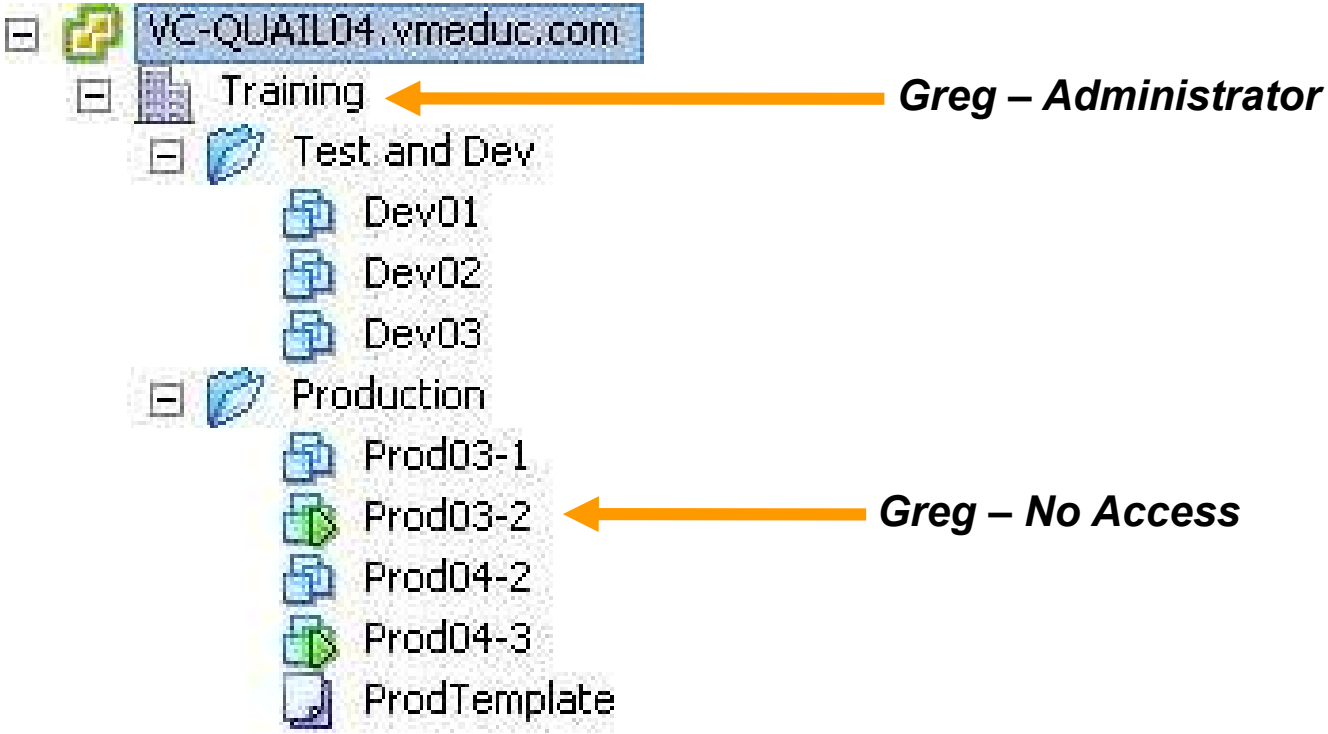
Viewing Roles and Assignments

- The **Roles** pane shows what users are assigned the selected role on a particular object.



Applying Permissions: Scenario 1

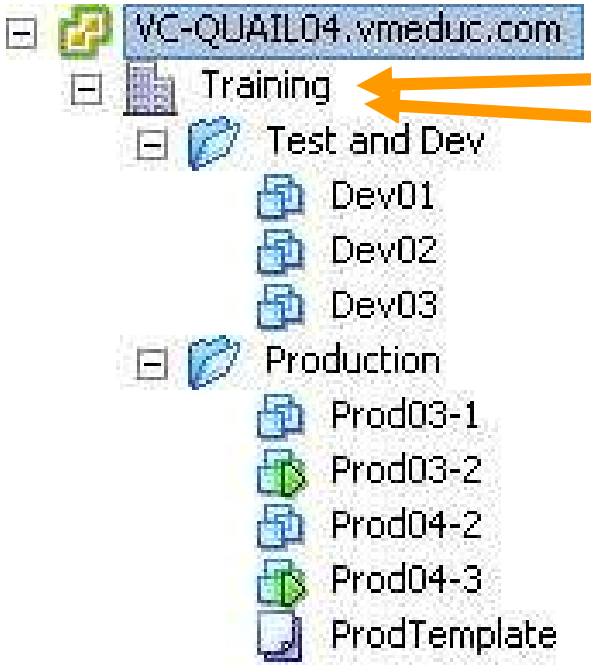
- A permission can propagate down the object hierarchy to all subobjects, or it can apply only to an immediate object.



Applying Permissions: Scenario 2

If a user is a member of multiple groups with permissions on the same object:

- The user is assigned the union of privileges assigned to the groups for that object.



Group1 – VM_Power_On (custom role)

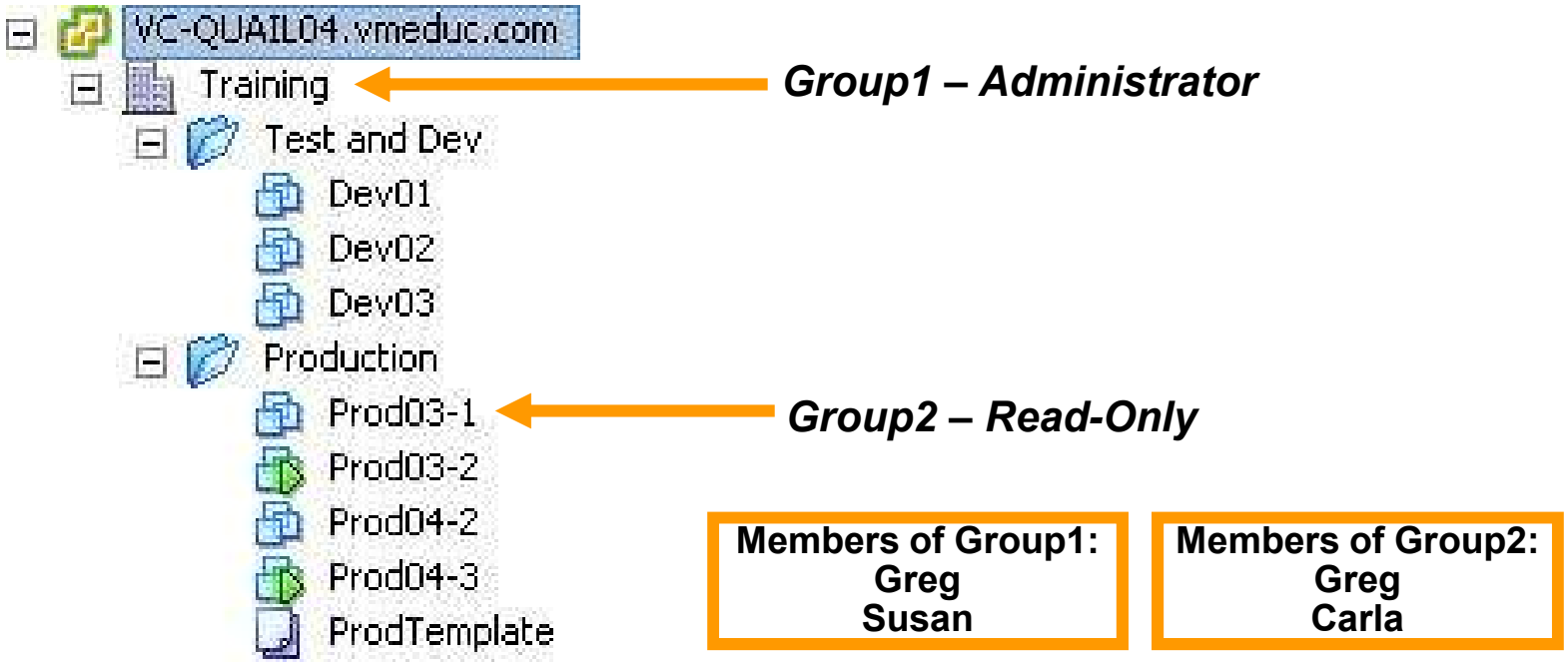
Group2 – Take_Snapshots (custom role)

Members of Group1:	Members of Group2:
Greg	Greg
Susan	Carla

Applying Permissions: Scenario 3

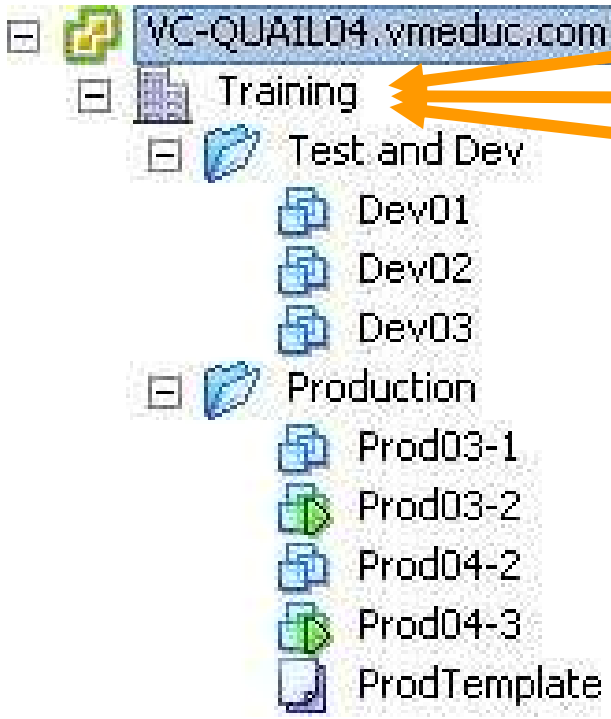
If a user is a member of multiple groups with permissions on different objects:

- For each object on which the group has permissions, the same permissions apply as if granted to the user directly.



Applying Permissions: Scenario 4

Permissions defined explicitly for the user on an object take precedence over all group permissions on that same object.



Group1 – VM_Power_On (custom role)

Group2 – Take_Snapshots (custom role)

Greg – Read-only

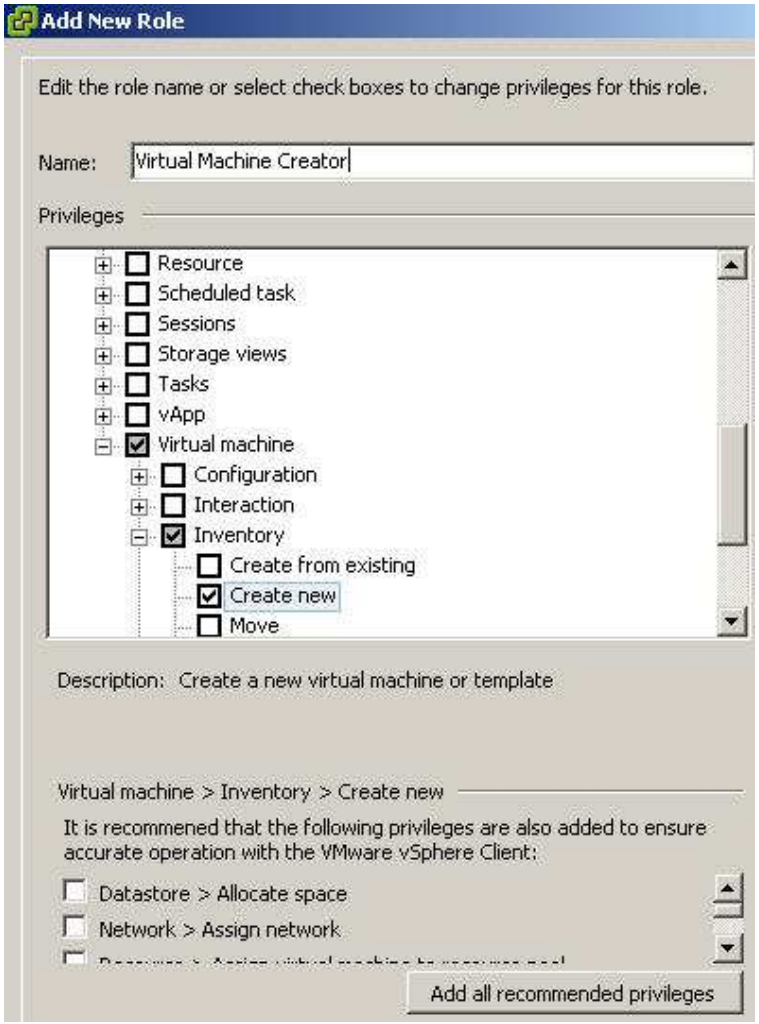
Members of Group1:
Greg
Susan

Members of Group2:
Greg
Carla

Creating a Role

To create a role:

1. Give it a descriptive name.
2. Select only the necessary privileges.



Creating a Role: Example

Create roles that enable only the necessary tasks.

- Example: Virtual Machine Creator

Use folders to contain the scope of permissions.

- For example, assign the Virtual Machine Creator role to user nancy and apply it to the Finance folder.

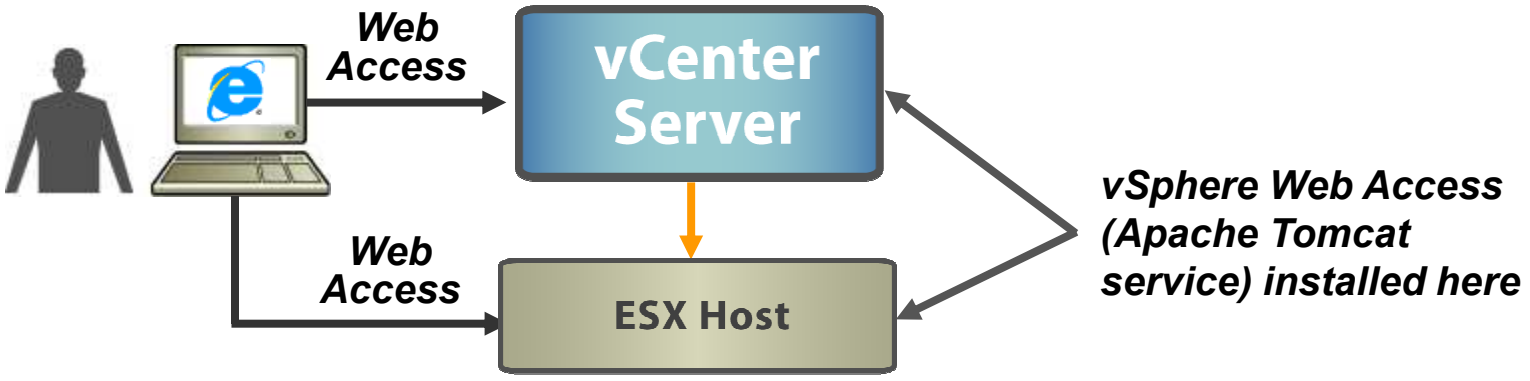
Virtual Machine Creator role

- Datastore > Allocate space
- Network > Assign network
- Resource > Assign virtual machine to resource pool
- Virtual machine > Inventory > Create new
- Virtual machine > Configuration > Add new disk
- Virtual machine > Configuration > Add or remove device

Access Control Using vSphere Web Access

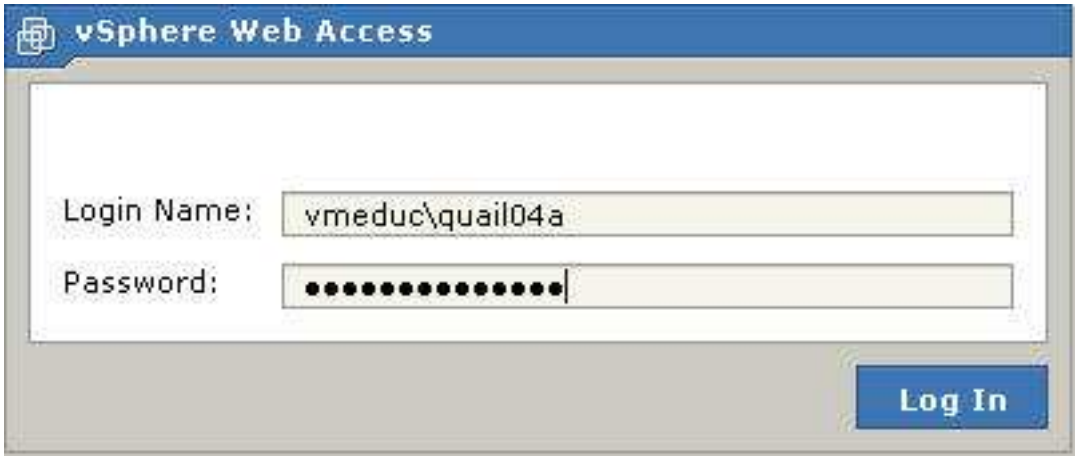
vSphere Web Access is a browser-based application that focuses on managing virtual machines.

- Administrators can provide end users browser-based access to virtual machines without having to install the VMware vSphere Client on their desktop.
- Client devices allow virtual machines to access media on the user's local floppy and CD/DVD drives.
  - Reduces the need to access these drives on the VMware ESX™ host

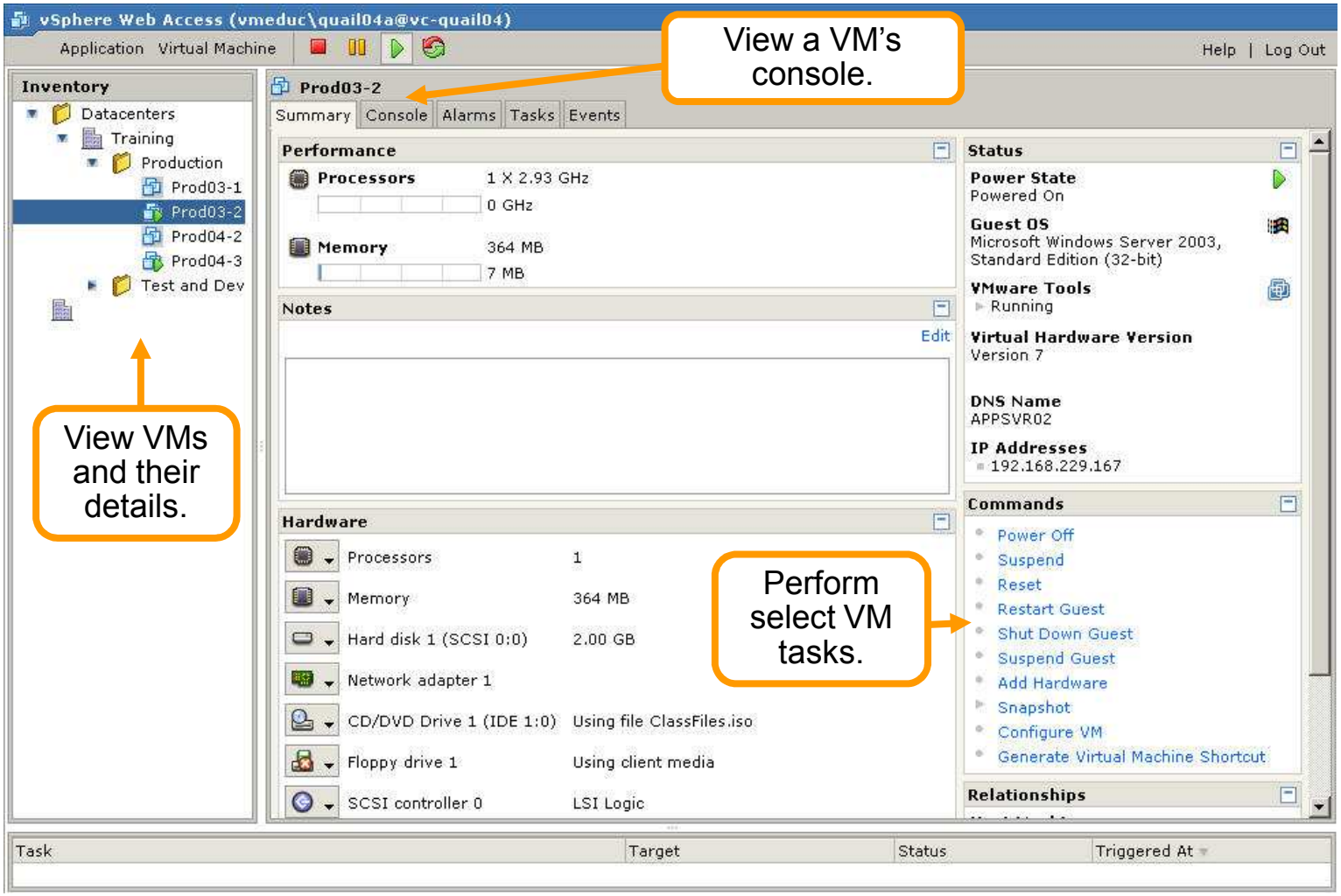


Using vSphere Web Access

1. Point Web browser to host name (or IP address) of vCenter Server system or ESX host, then click the Log in to Web Access link.
   - vSphere Web Access is not available on ESXi hosts.
2. Log in to vSphere Web Access.

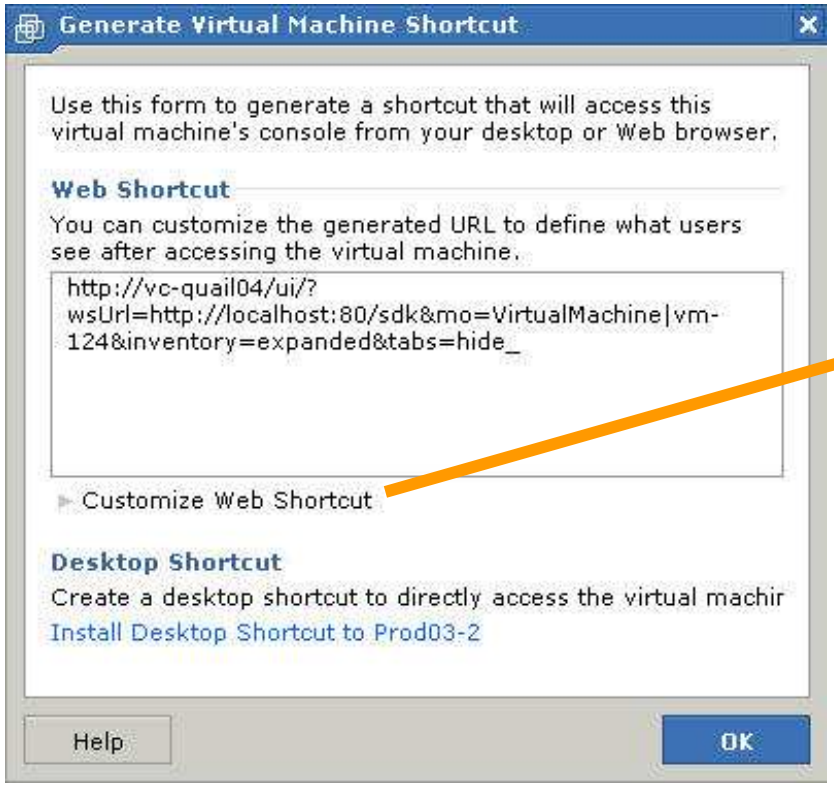


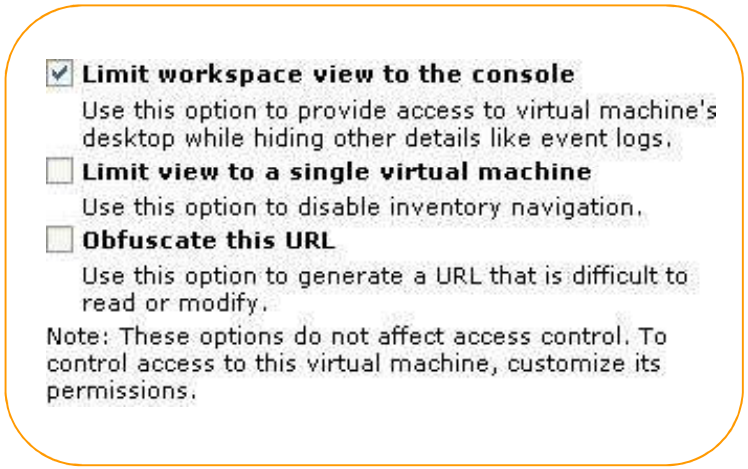
vSphere Web Access Tasks



Generating Virtual Machine Shortcut

- Way to provide access to a virtual machine through a URL
- Useful for including in an email message





Lab 14

In this lab, you will create vCenter Server user permissions.

- Create a Windows account on the vCenter Server system.
- Create the Virtual Machine Creator role.
- Assign the role to a user.
- Verify that the user can create a virtual machine.
- Restrict virtual machine creation to the local datastore only.
- (Optional) Create a role named Template Deployer.

Key Points

- A permission is a user/group+role combination that is applied to an object in the inventory.
- A permission can propagate down the object hierarchy to all subobjects, or it can apply only to an immediate object.
- As a best practice, define a role using the smallest number of privileges possible for better security and added control.
- vSphere Web Access can be used to provide end users with browser-based access to virtual machines without the need to install the vSphere Client on their desktops.