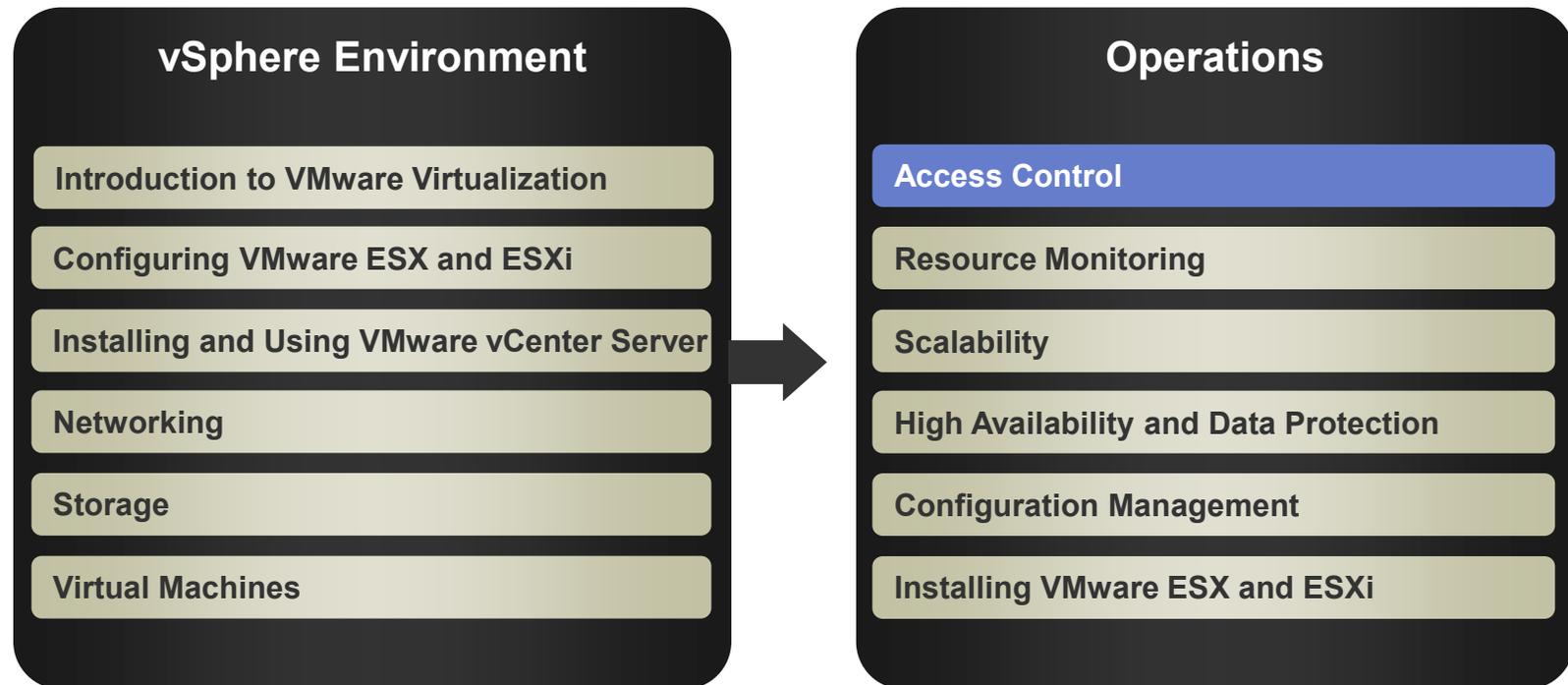




Access Control

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

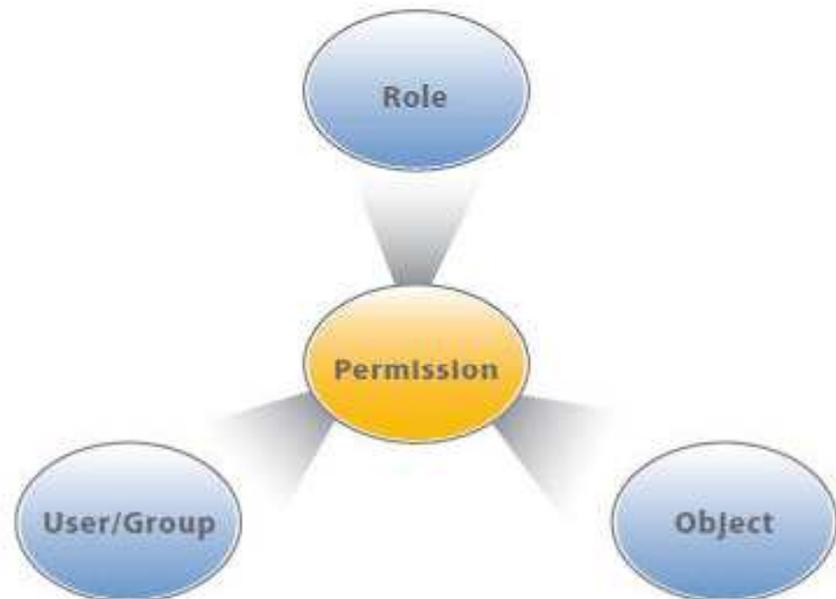
Access Control Overview

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

Key concepts:

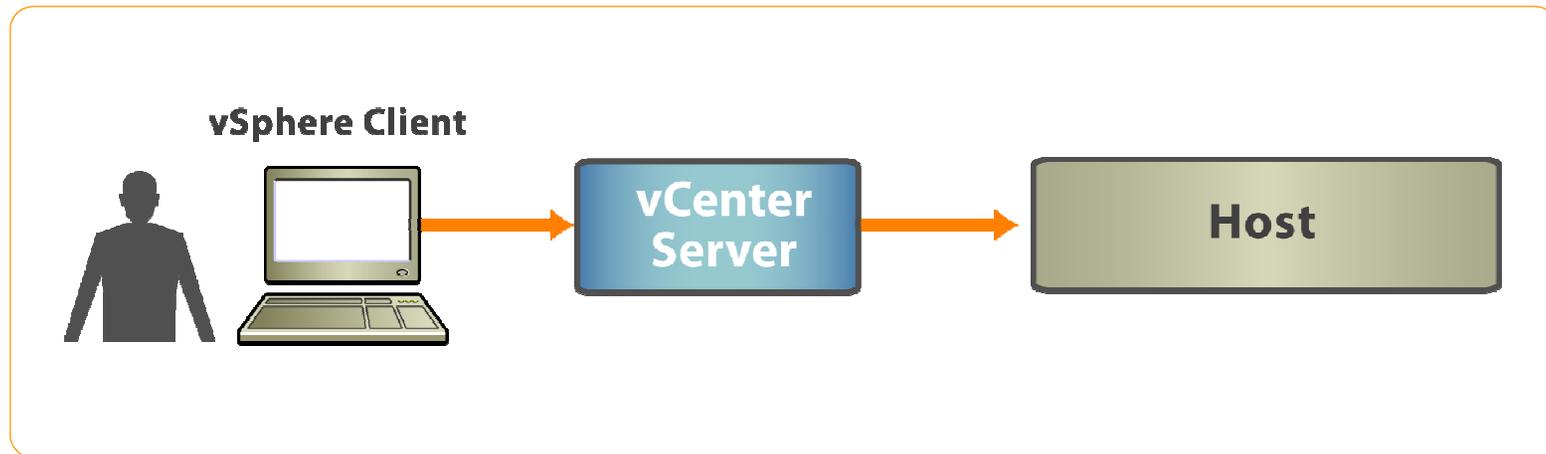
- > Privilege – Defines an action that can be performed
- > Role – A set of privileges
- > Object – The target of the action
- > Windows user/group – Indicates who can perform the action

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.

Roles

Name
No access
Read-only
Administrator
Virtual machine power user (sample)
Virtual machine user (sample)
Resource pool administrator (sample)
VMware Consolidated Backup user (sample)
Datastore consumer (sample)
Network consumer (sample)

Name: Virtual machine user (sample)

Privileges

- All Privileges
 - Alarms
 - Datacenter
 - Datastore
 - Distributed virtual port group
 - Distributed Virtual Switch
 - Extension
 - Folder
 - Global
 - Host
 - Host profile
 - Network
 - Performance
 - Permissions
 - Resource
 - Scheduled task
 - Sessions
 - Storage views
 - Tasks
 - vApp
 - Virtual machine

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.

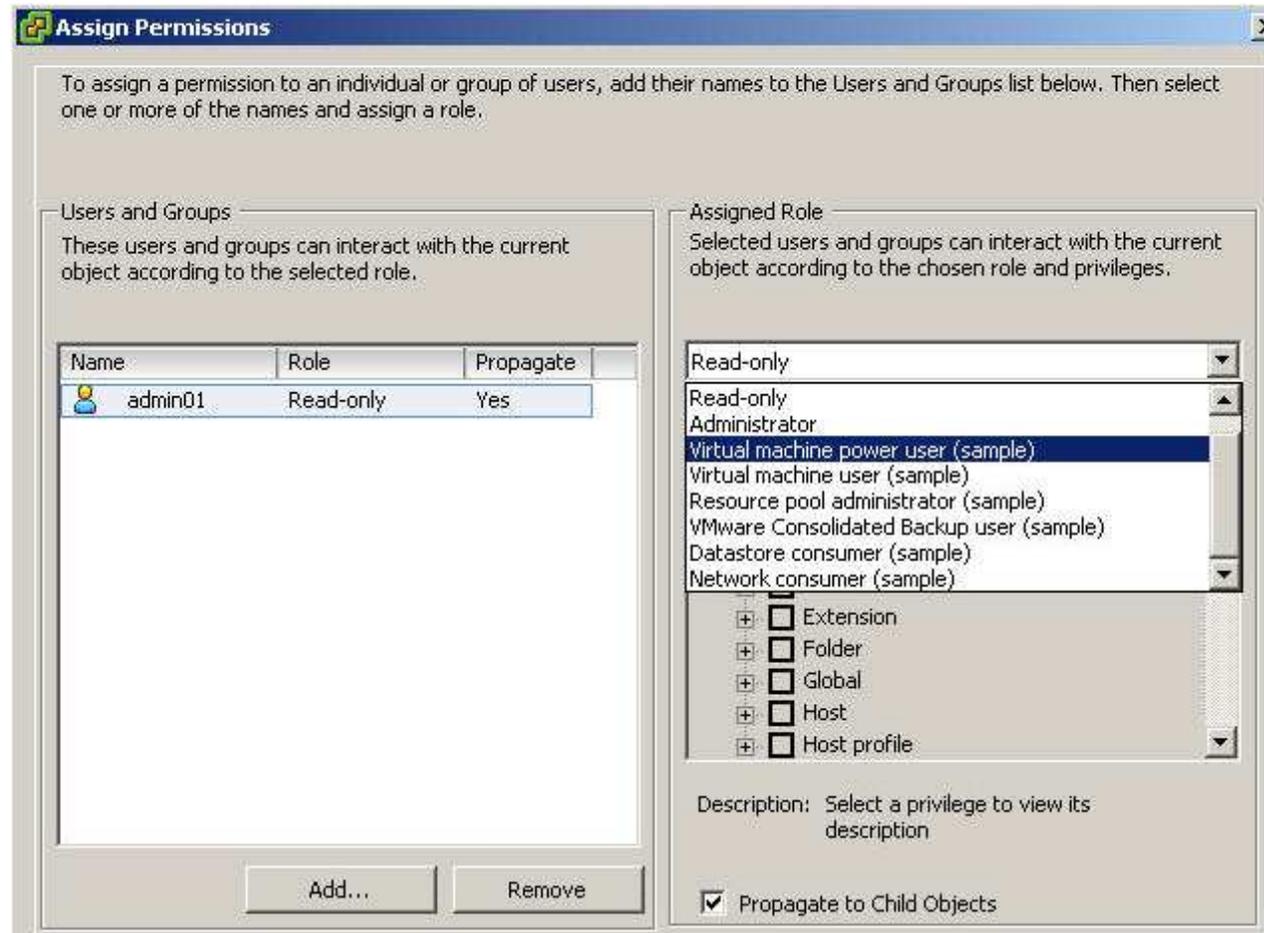


The screenshot displays the VMware vSphere interface. On the left, a tree view shows the hierarchy: VC-GOOSE06 > Training > Lab Servers > Lab Cluster. The Lab Cluster contains several objects: sc-goose06, sc-goose07, Prod07-1, Prod07-2, and Test03-1. The main pane shows the 'Lab Servers' object selected, with the 'Permissions' tab active. The Permissions tab displays a table of users and groups with their roles and where they are defined.

User/Group	Role	Defined in
vmadmin01a	Virtual machine power user (sample)	Training
vcadmin01a	Administrator	VC-GOOSE06
Administrators	Administrator	VC-GOOSE06

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.

Roles

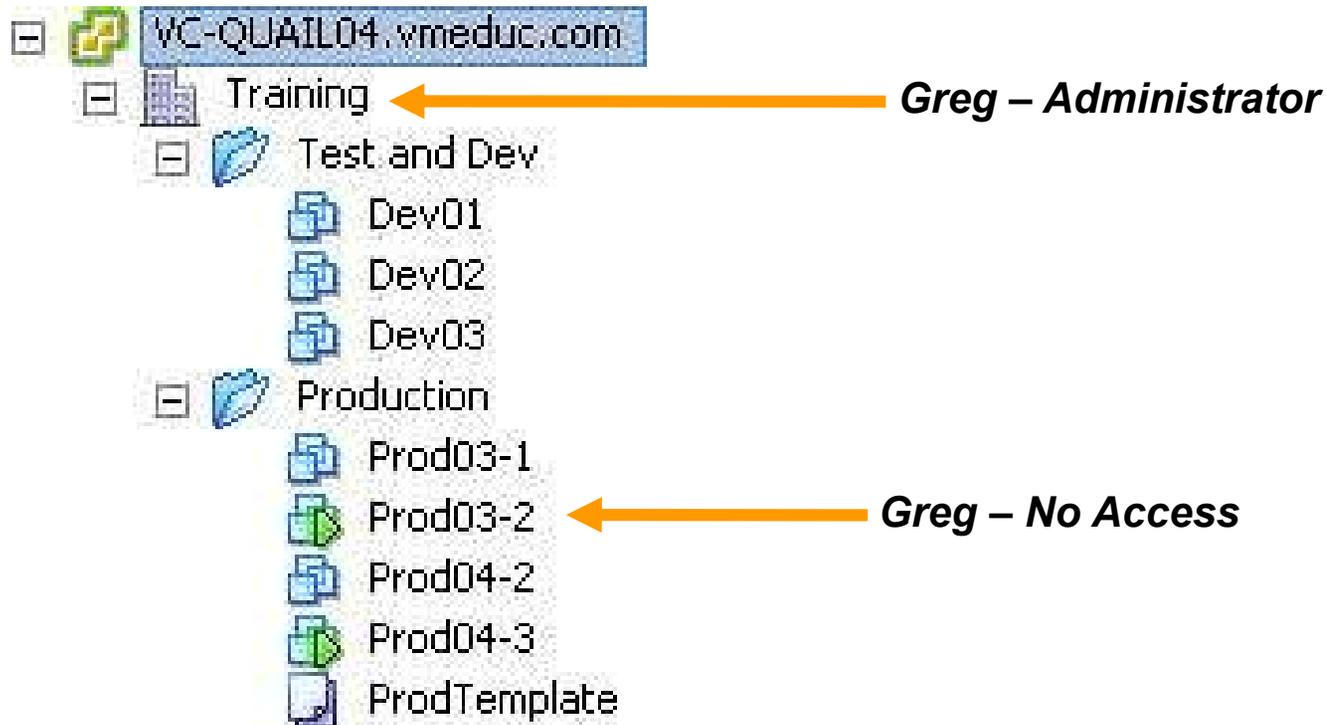
Name
No access
Read-only
Administrator
Virtual machine power user (sample)
Virtual machine user (sample)
Resource pool administrator (sample)
VMware Consolidated Backup user (sample)
Datastore consumer (sample)
Network consumer (sample)
Virtual machine administrator

Usage: Administrator

- [-] Datacenters
 - Administrators
 - vcadmin01a

Applying Permissions: Scenario 1

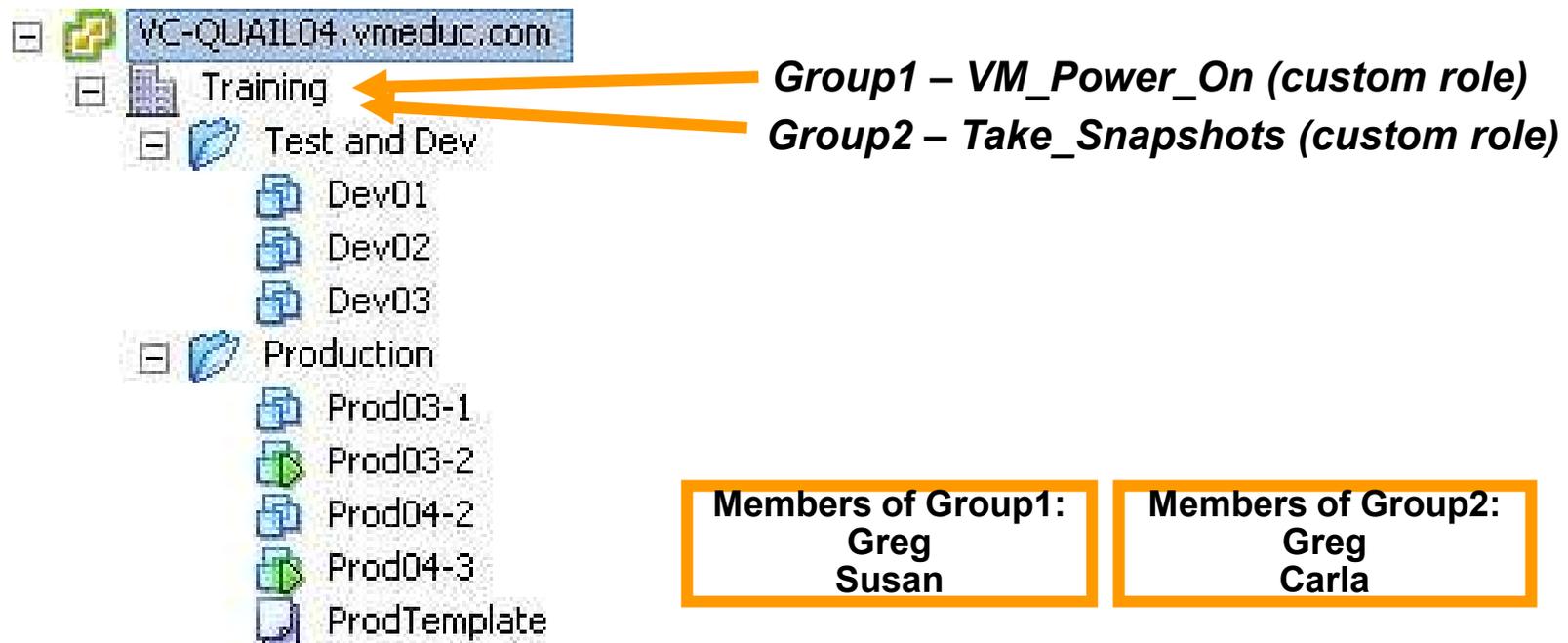
- A permission can propagate down the object hierarchy to all subobjects, or it can apply only to an immediate object.



Applying Permissions: Scenario 2

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

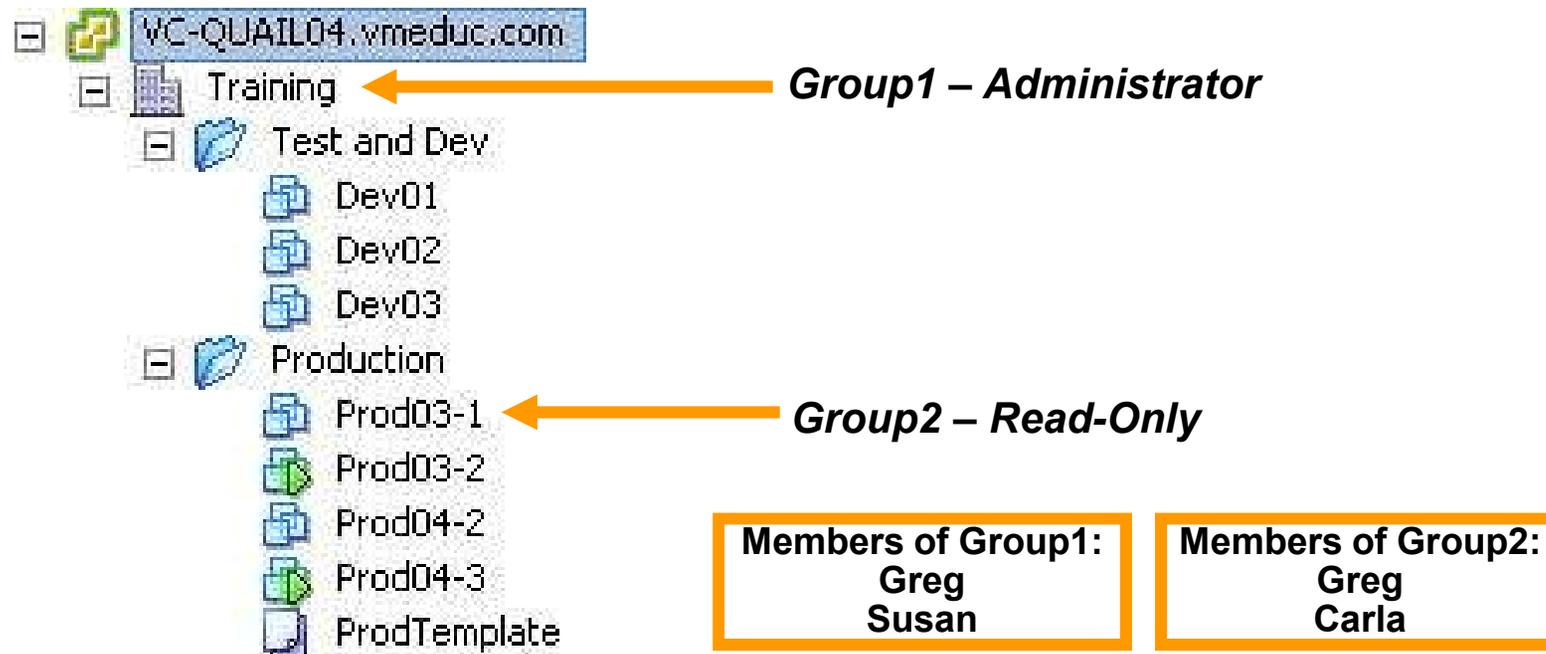
- The user is assigned the union of privileges assigned to the groups for that object.



Applying Permissions: Scenario 3

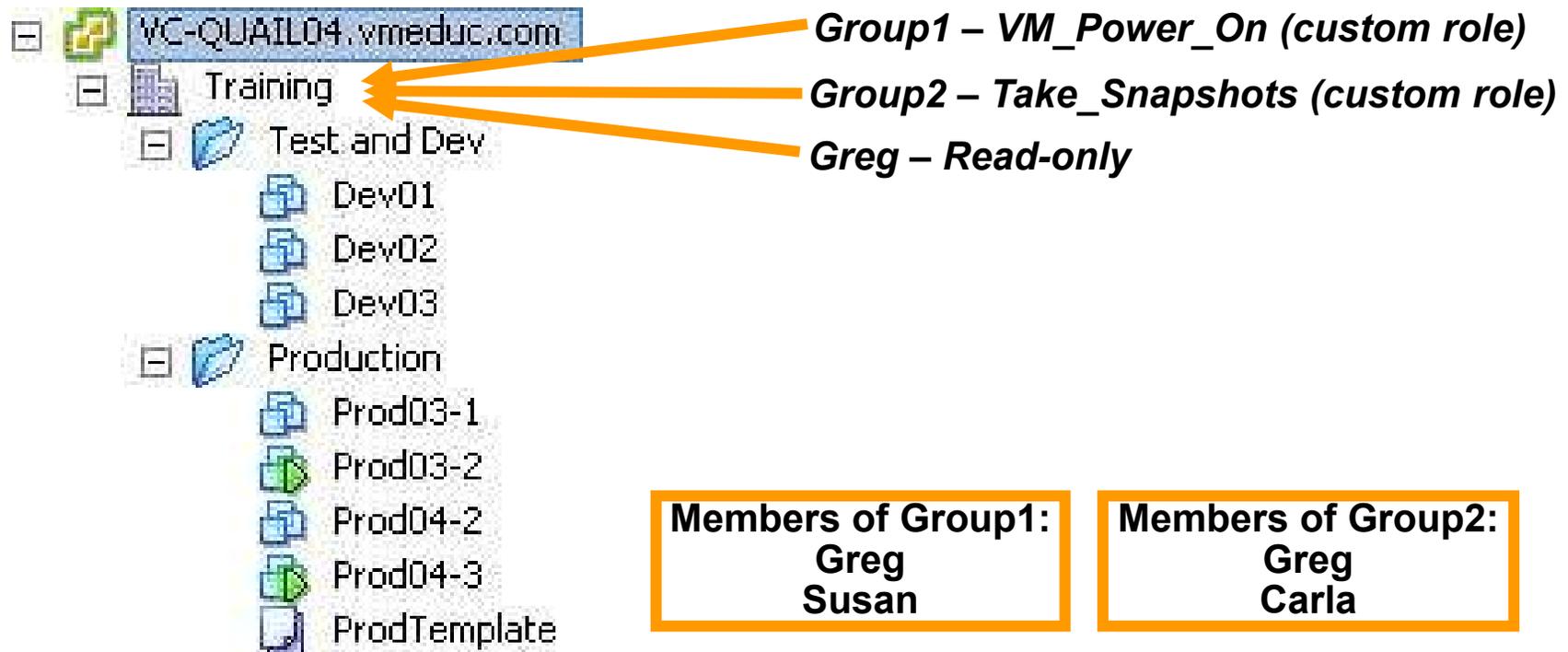
If a user is a member of multiple groups with permissions on different objects:

- 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.



Creating a Role

To create a role:

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

Add New Role

Edit the role name or select check boxes to change privileges for this role.

Name:

Privileges

- Resource
- Scheduled task
- Sessions
- Storage views
- Tasks
- vApp
- Virtual machine
 - Configuration
 - Interaction
 - Inventory
 - Create from existing
 - Create new
 - Move

Description:

Virtual machine > Inventory > Create new

It is recommended that the following privileges are also added to ensure accurate operation with the VMware vSphere Client:

- Datastore > Allocate space
- Network > Assign network

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.

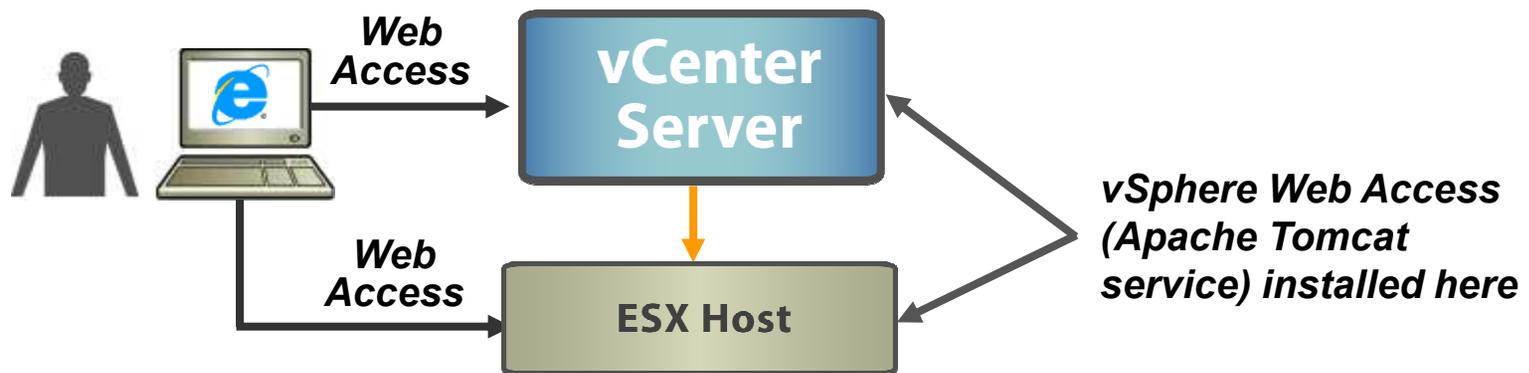
Virtual Machine Creator role

- > 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

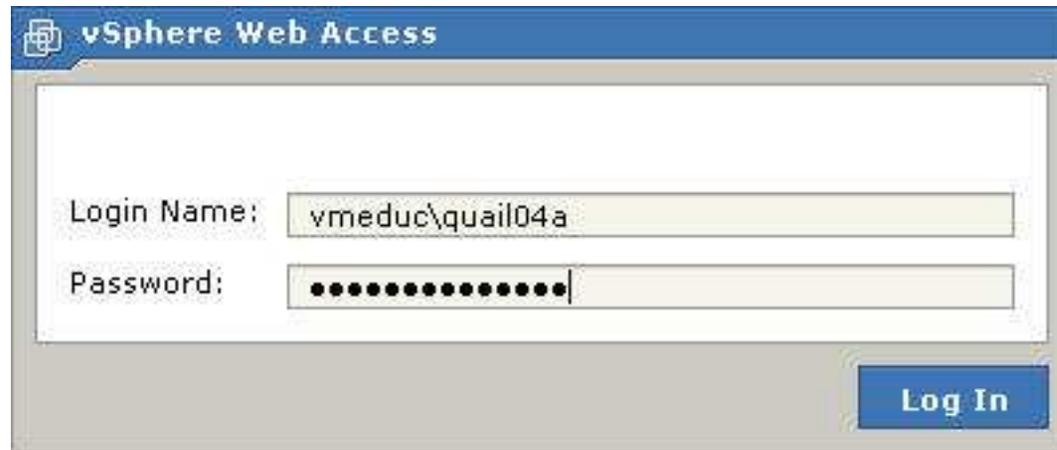
vSphere Web Access is a browser-based application that focuses on managing virtual machines.

- 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.



The screenshot shows the vSphere Web Access login window. The title bar reads "vSphere Web Access". Below the title bar, there are two input fields: "Login Name:" with the text "vmeduc\quail04a" and "Password:" with a masked password represented by a series of black dots. A blue "Log In" button is located at the bottom right of the form.

vSphere Web Access Tasks

The screenshot displays the vSphere Web Access interface for a virtual machine named 'Prod03-2'. The interface is divided into several sections:

- Inventory:** A tree view on the left showing the hierarchy of datacenters, training, production, and test/dev environments. 'Prod03-2' is selected.
- Summary:** A central pane with tabs for Summary, Console, Alarms, Tasks, and Events. The Summary tab is active, showing performance metrics (Processors: 1 x 2.93 GHz, Memory: 364 MB) and hardware details (Processors: 1, Memory: 364 MB, Hard disk 1: 2.00 GB, Network adapter 1, CD/DVD Drive 1, Floppy drive 1, SCSI controller 0).
- Status:** A right-hand pane showing the VM's power state (Powered On), guest OS (Microsoft Windows Server 2003), VMware Tools (Running), and virtual hardware version (Version 7).
- Commands:** A list of actions available for the VM, including Power Off, Suspend, Reset, Restart Guest, Shut Down Guest, Suspend Guest, Add Hardware, Snapshot, Configure VM, and Generate Virtual Machine Shortcut.

Three callout boxes with orange borders and arrows highlight key features:

- View a VM's console.** Points to the 'Console' tab in the Summary pane.
- View VMs and their details.** Points to the 'Prod03-2' entry in the Inventory tree.
- Perform select VM tasks.** Points to the 'Commands' list on the right.

Task	Target	Status	Triggered At
------	--------	--------	--------------

Generating Virtual Machine Shortcut

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

Generate Virtual Machine Shortcut

Use this form to generate a shortcut that will access this virtual machine's console from your desktop or Web browser.

Web Shortcut

You can customize the generated URL to define what users see after accessing the virtual machine.

`http://vc-quail04/ui/?wsUrl=http://localhost:80/sdk&mo=VirtualMachine|vm-124&inventory=expanded&tabs=hide_`

▶ Customize Web Shortcut

Desktop Shortcut

Create a desktop shortcut to directly access the virtual machir

[Install Desktop Shortcut to Prod03-2](#)

Help OK

- Limit workspace view to the console**
Use this option to provide access to virtual machine's desktop while hiding other details like event logs.
 - Limit view to a single virtual machine**
Use this option to disable inventory navigation.
 - Obfuscate this URL**
Use this option to generate a URL that is difficult to read or modify.
- Note: These options do not affect access control. To control access to this virtual machine, customize its permissions.

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.