

액세스 및 인증 제어

중요성

다중사용자가 VMware vSphere® 환경에 접근시 각 사용자에게 필요한 사용 권한만 제공하고 그 이상의 권한은 제공하지 않는 것이 바람직합니다. VMware® vCenter Server™를 사용하면 사용 권한 할당을 유연하게 운영할 수 있습니다.

1.ESXi 호스트 액세스 및 인증 구성

2.역할 및 사용 권한 구성

1.ESXi 호스트 접근 및 인증 구성

학습 목표

이 과정을 마치고 나면 다음을 수행할 수 있습니다.

- 서비스를 사용/사용하지 않도록 설정하여 VMware vSphere® ESXi™ 방화벽을 구성합니다.
- ESXi 호스트에서 잠금 모드를 사용/사용하지 않도록 설정합니다.
- 디렉토리 서비스를 사용하여 인증하도록 사용자 로그인을 구성합니다.

보안 프로파일 서비스 구성

The screenshot illustrates the configuration of a security profile service in a vSphere environment. The main window shows the 'Security Profile' tab, with the 'Services' section expanded. The 'I/O Redirector (Active Directory Service)' is highlighted in the list. The 'Services Properties' dialog is open, showing the 'I/O Redirector (Active Directory Service) (Iwiod) Options' sub-dialog. The 'Startup Policy' is set to 'Start and stop manually', and the 'Service Commands' section shows the 'Start' button. A blue arrow points from the 'Options...' button in the 'Services Properties' dialog to the 'I/O Redirector (Active Directory Service) (Iwiod) Options' dialog.

Security Profile

Services

- I/O Redirector (Active Directory Service)
- Network Login Server (Active Directory Service)
- NTP Daemon
- vpix
- Local Security Authentication Server (Active Directory Service)
- ESXShell
- lbttd
- SSH
- Direct Console UI
- CIM Server

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Power Management
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- Security Profile**

Services Properties

Remote Access

By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts. Unless configured otherwise, daemons will start automatically.

Label	Daemon
I/O Redirector (Active Directory Se...	Stopped
Network Login Server (Active Direct...	Stopped
lbttd	Running
vpix	
ESX Shell	
Local Security Authentica...	
NTP Daemon	
SSH	
Direct Console UI	
CIM Server	

I/O Redirector (Active Directory Service) (Iwiod) Options

Status: Stopped

Startup Policy:

- ☐ Start automatically if any ports are open, and stop when all ports are closed
- ☐ Start and stop with host
- ☒ Start and stop manually

Service Commands:

Start Stop Restart

OK Cancel Help

ESXi 방화벽 구성

The image shows the ESXi configuration interface with several components highlighted and annotated:

- Software List:** A list of configuration options on the left, with **Security Profile** circled in blue.
- Firewall Section:** The **Firewall** section is circled in blue in the top navigation pane.
- Refresh and Properties...:** The **Refresh** and **Properties...** buttons are circled in blue.
- Firewall Properties Dialog:** A dialog box titled **Firewall Properties** is open, showing the **Remote Access** tab. It contains a table of services and their configurations.
- Firewall Settings Dialog:** A dialog box titled **Firewall Settings** is open, showing the **Allowed IP Addresses** section. It has two radio buttons: **Allow connections from any IP address** (selected) and **Only allow connections from the following networks:** (unselected). Below the second option is a text box for entering IP addresses and a note: "Separate each network with a comma. Example: 192.168.0.0/24, 192.168.1.2, 2001::1/64, fd3e:29a6:0a81:e478::/64".
- Annotations:** A blue arrow points from the **Firewall...** button in the **Firewall Properties** dialog to the **Firewall Settings** dialog.

Firewall Properties Dialog - Remote Access Tab

Label	Incoming Ports	Outgoing Ports	Protocols	Daemon
Required Services				
Secure Shell				
<input checked="" type="checkbox"/> SSH Server	22		TCP	Stopped
<input type="checkbox"/> SSH Client		22	TCP	N/A
Simple Network Management Protocol				
Ungrouped				
<input checked="" type="checkbox"/> DNS Client	53	53	UDP	N/A
<input type="checkbox"/> VM serial port connected to vSPC		0-65535	TCP	N/A
<input checked="" type="checkbox"/> NTP Client		123	UDP	Running
<input checked="" type="checkbox"/> Fault Tolerance	8100,8200	80,8100,8200	TCP,UDP	N/A

Firewall Settings Dialog - Allowed IP Addresses

Allowed IP Addresses

☒ Allow connections from any IP address

☐ Only allow connections from the following networks:

Separate each network with a comma.
Example:
192.168.0.0/24, 192.168.1.2, 2001::1/64, fd3e:29a6:0a81:e478::/64

OK Cancel Help

잠금 모드 활성화 및 비활성화

The image shows a vSphere configuration interface for a host named 'esxi01.vclass.local'. The 'Configuration' tab is selected, and the 'Lockdown Mode' section is highlighted. The 'Lockdown Mode' is currently set to 'Disabled'. A blue arrow points from the 'Edit...' button to a terminal window titled 'esxi01.vclass.local - PuTTY'. The terminal shows a login attempt as 'root' which is denied, and a password prompt is visible.

Configuration Issues
SSH for the host has been enabled

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Power Management
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- ▶ Security Profile

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through local console or an authorized centralized management application.

Lockdown Mode: Disabled

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through local console or an authorized centralized management application.

If you are unsure what to do, leave this box unchecked.

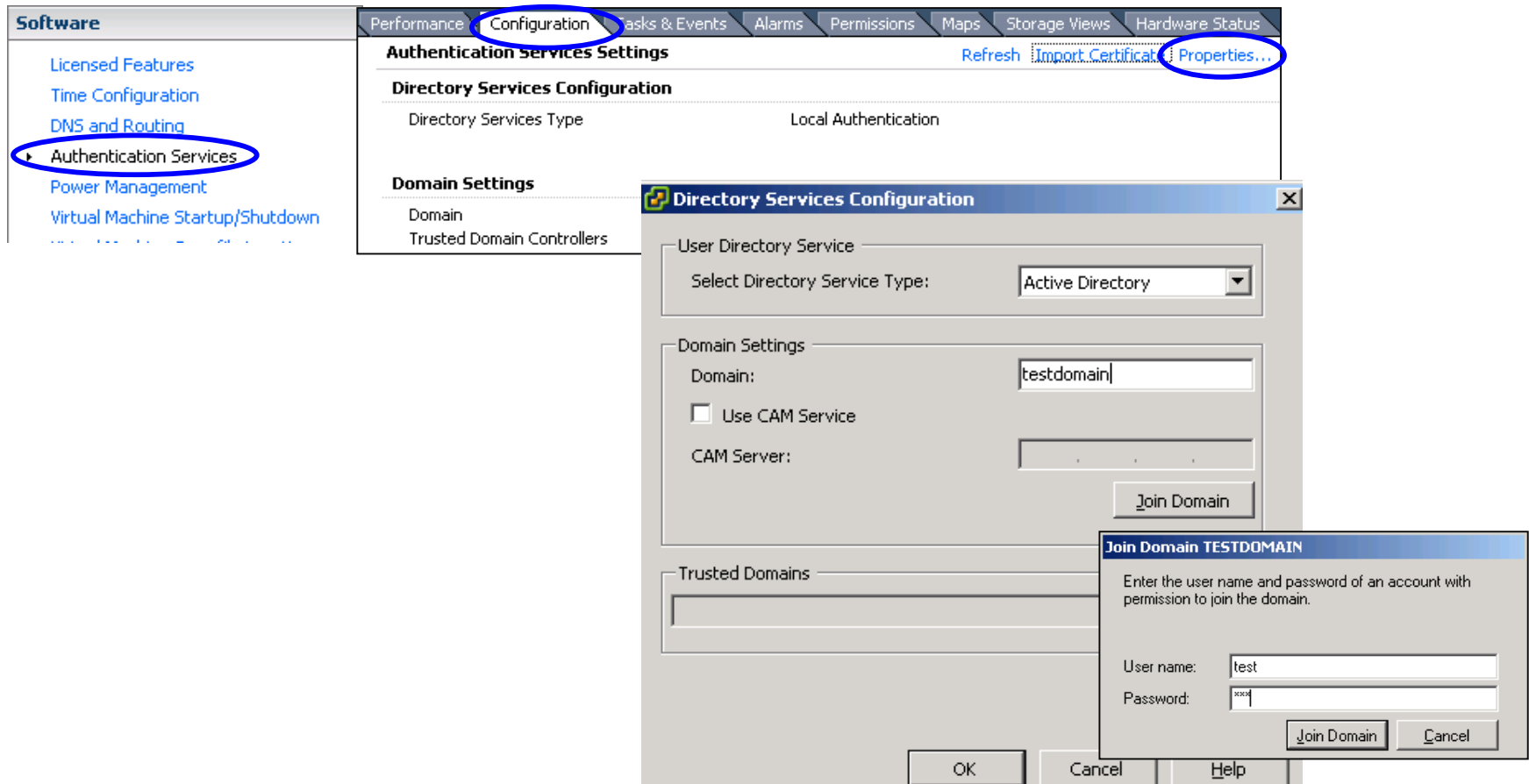
☒ Enable Lockdown Mode

OK Cancel Help

esxi01.vclass.local - PuTTY

```
login as: root
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password: █
```


Active Directory로 ESXi 통합



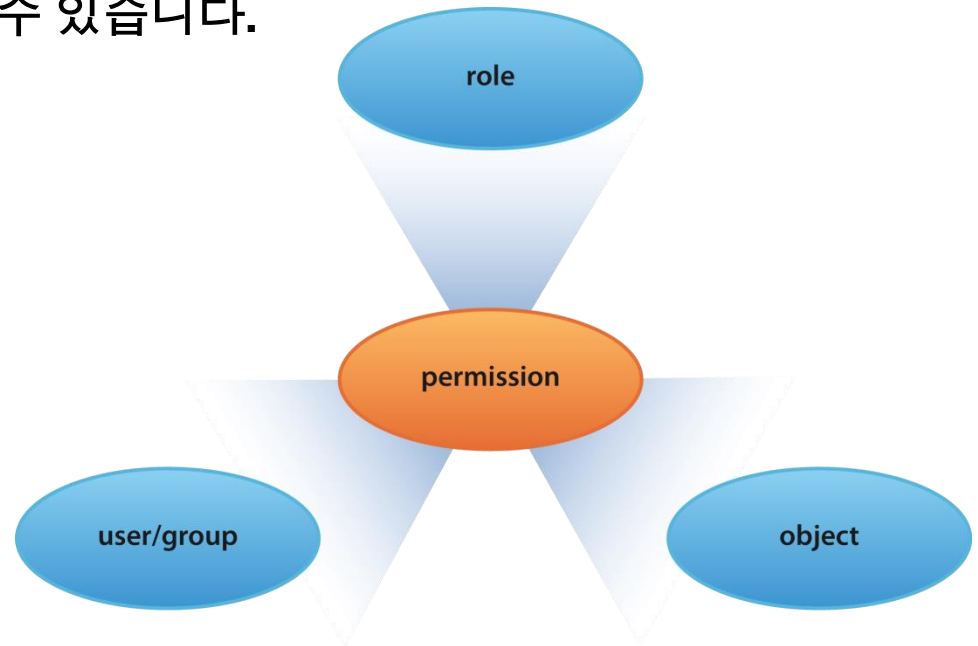
2. 역할 및 사용 권한 구성

액세스 제어 개요

액세스 제어 시스템을 사용하여 vCenter Server 관리자는 인벤토리의 객체에 액세스할 수 있는 사용자의 권한을 정의할 수 있습니다.

핵심 개념:

- 권한 – 수행할 수 있는 작업을 정의함
- 역할 – 권한 세트
- 객체 – 작업 대상
- 사용자/그룹 – 작업을 수행할 수 있는 사람을 표시함



역할, 사용자 또는 그룹 및 객체 모두 사용 권한을 정의합니다.

사용자 및 그룹

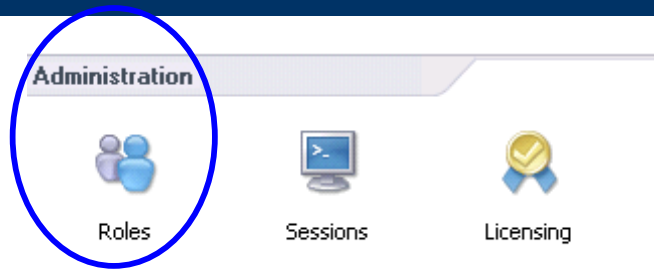
vCenter Server 또는 ESXi 사용자/그룹은 로컬 사용자 또는 AD(Active Directory) 도메인 사용자일 수 있습니다.

AD 서비스는 모든 로컬 서비스에 인증을 제공합니다.

- VMware vSphere® Client™
- 다이렉트 콘솔 사용자 인터페이스
- 기술 지원 모드(로컬 및 원격)
- VMware vSphere® API를 통한 액세스

AD 그룹 ESX Admins에 있는 사용자는 관리자 역할을 자동으로 할당 받습니다.

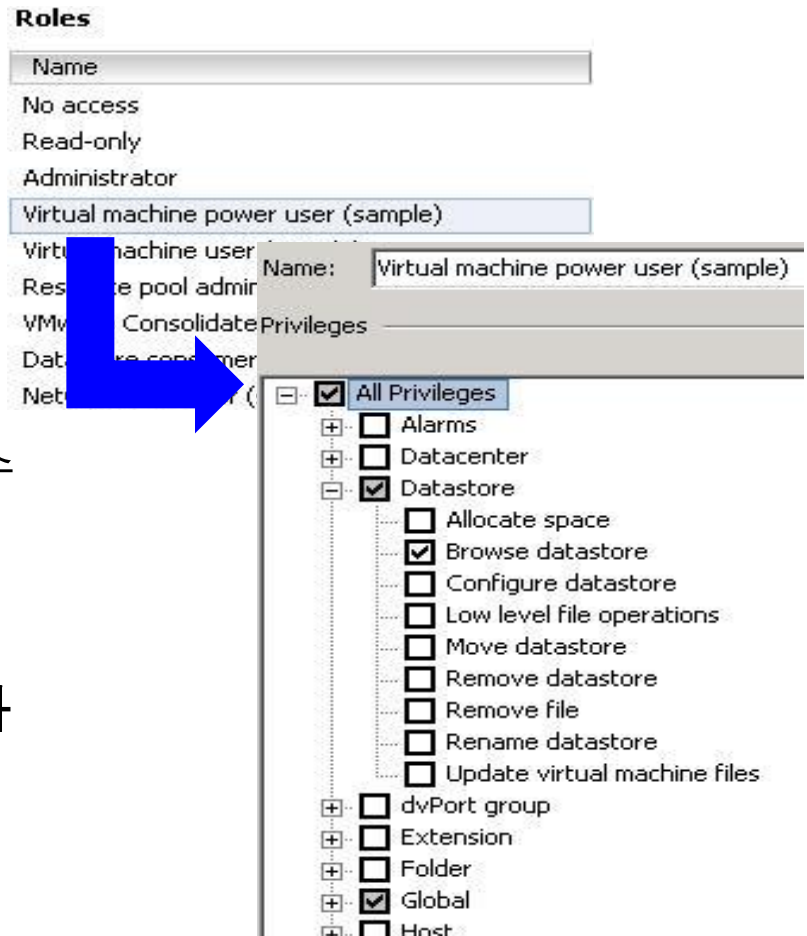
역할



역할은 권한의 모음입니다.

- 사용자는 역할을 통해 작업을 수행할 수 있습니다.
- 역할은 범주로 그룹화됩니다.

역할에는 시스템 역할, 샘플 역할 및 사용자 지정 기본 역할이 포함됩니다.



객체

객체는 수행되는 작업에 대한 엔터티입니다.

- 객체에는 데이터 센터, 폴더, 리소스 풀, 클러스터, 호스트, 데이터스토어, 네트워크 및 가상 머신이 포함됩니다.

모든 객체에는 Permissions(사용 권한) 탭이 있습니다.

- 이 탭에는 선택한 객체와 연결된 사용자 또는 그룹 및 역할을 표시됩니다.

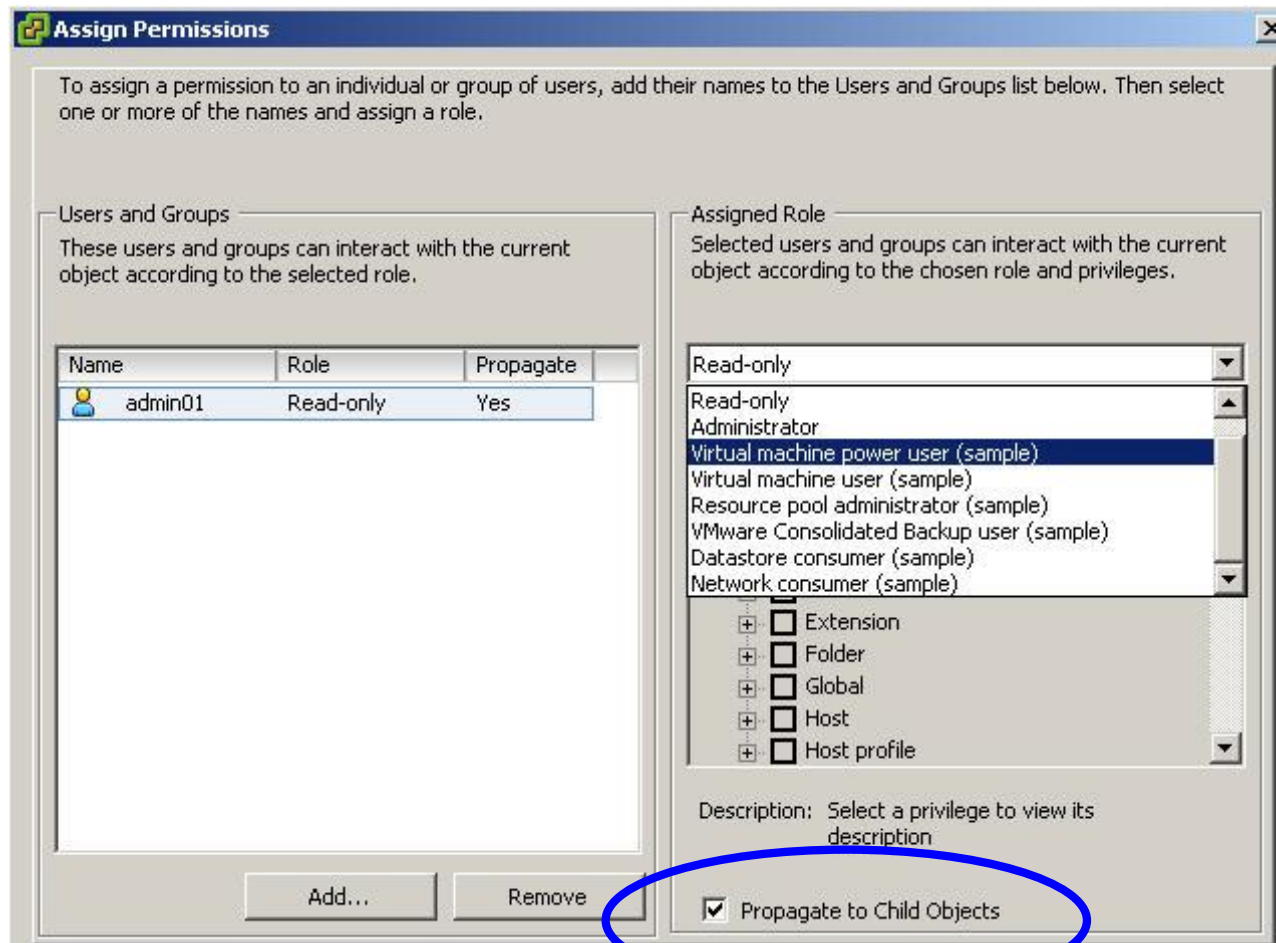


User/Group	Role	Defined in
vmadmin01a	Virtual machine power user (sample)	Training
vcadmin01a	Administrator	VC-GOOSE06
Administrators	Administrator	VC-GOOSE06

사용 권한 할당

사용 권한을 할당하려면

1. 사용자를 선택합니다.
2. 역할을 선택합니다.
3. (선택 사항) 하위 객체로 사용 권한을 전파합니다.



역할 및 할당 보기

Roles(역할) 창은 특정 객체에 선택된 역할을 할당한 사용자를 표시합니다.

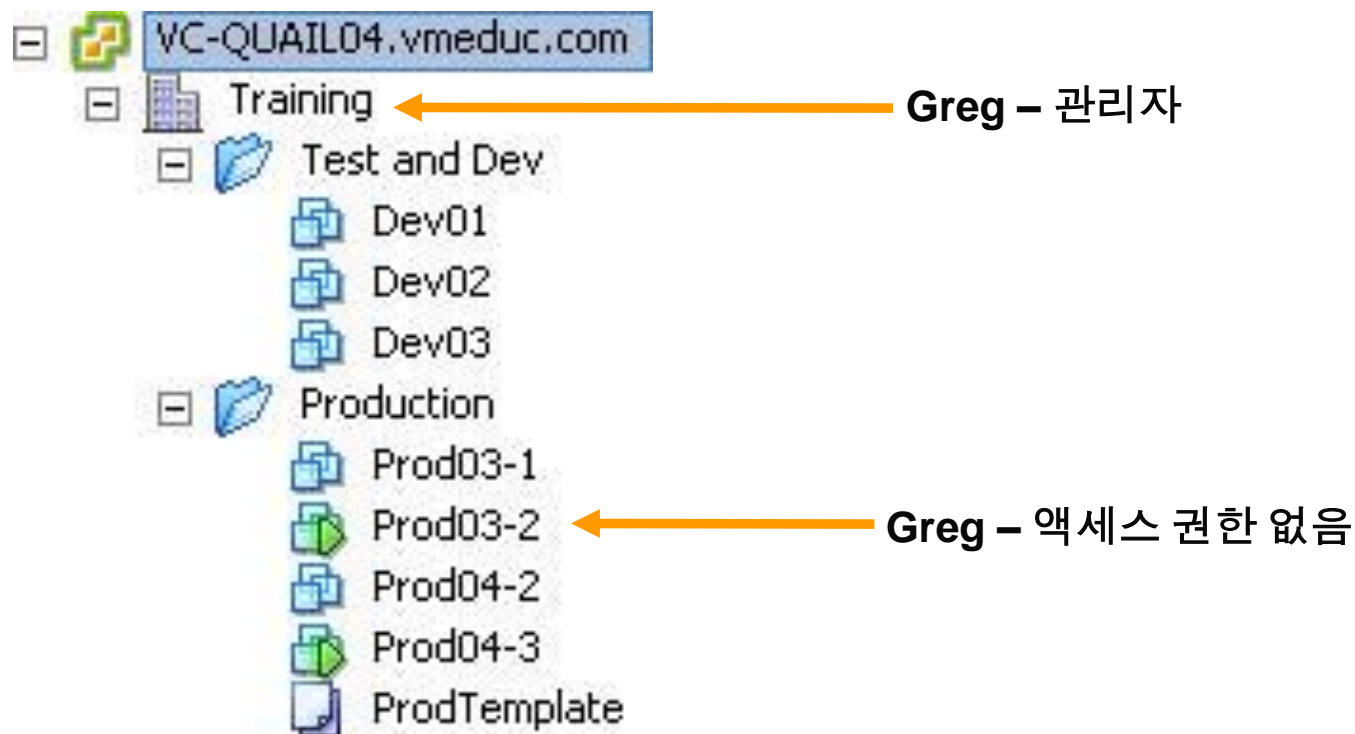
Roles

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)
vm-creator-Andrew

Usage: vm-creator-Andrew

사용 권한 적용 시나리오 1

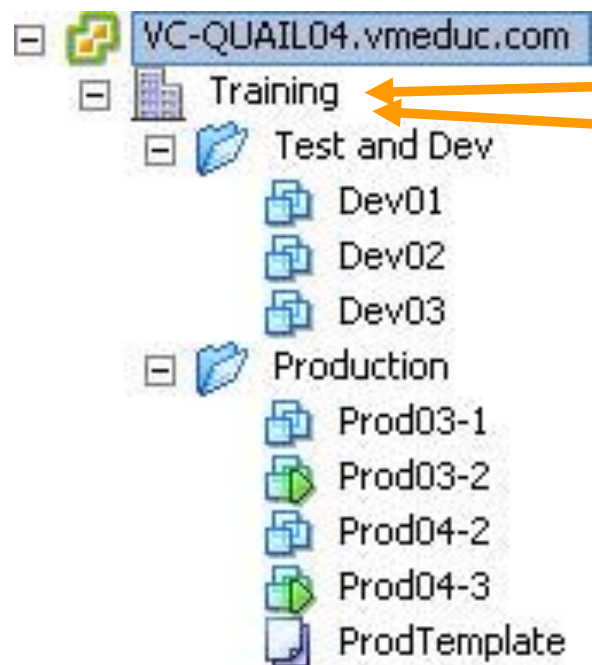
사용 권한은 객체를 모든 하위 객체로 계층적으로 전파하거나 임시 객체에
만 적용할 수 있습니다.



사용 권한 적용 시나리오 2

사용자가 동일한 객체에 대한 사용 권한을 가진 여러 그룹의 구성원일 경우,

- 사용자는 해당 객체의 그룹에 할당된 통합 권한을 할당 받습니다.



Group1 – VM_Power_On(사용자 지정 역할)

Group2 – Take_Snapshots(사용자 지정 역할)

Group1의 구성원:

Greg
Susan

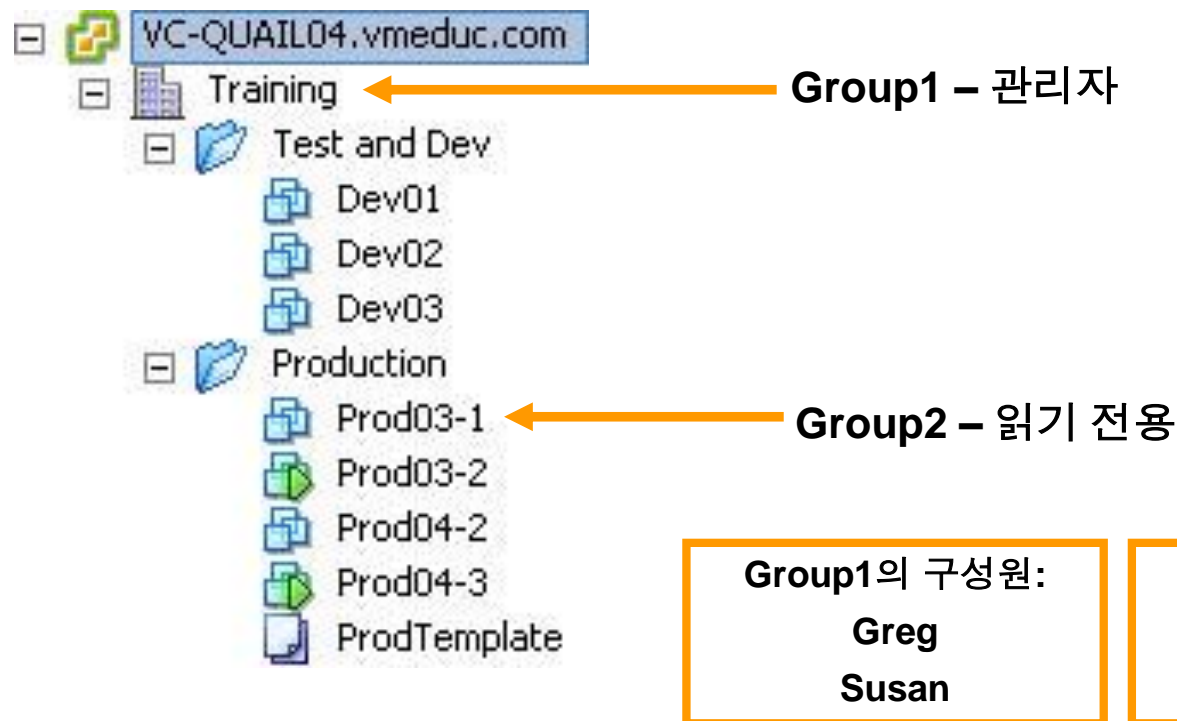
Group2의 구성원:

Greg
Carla

사용 권한 적용 시나리오 3

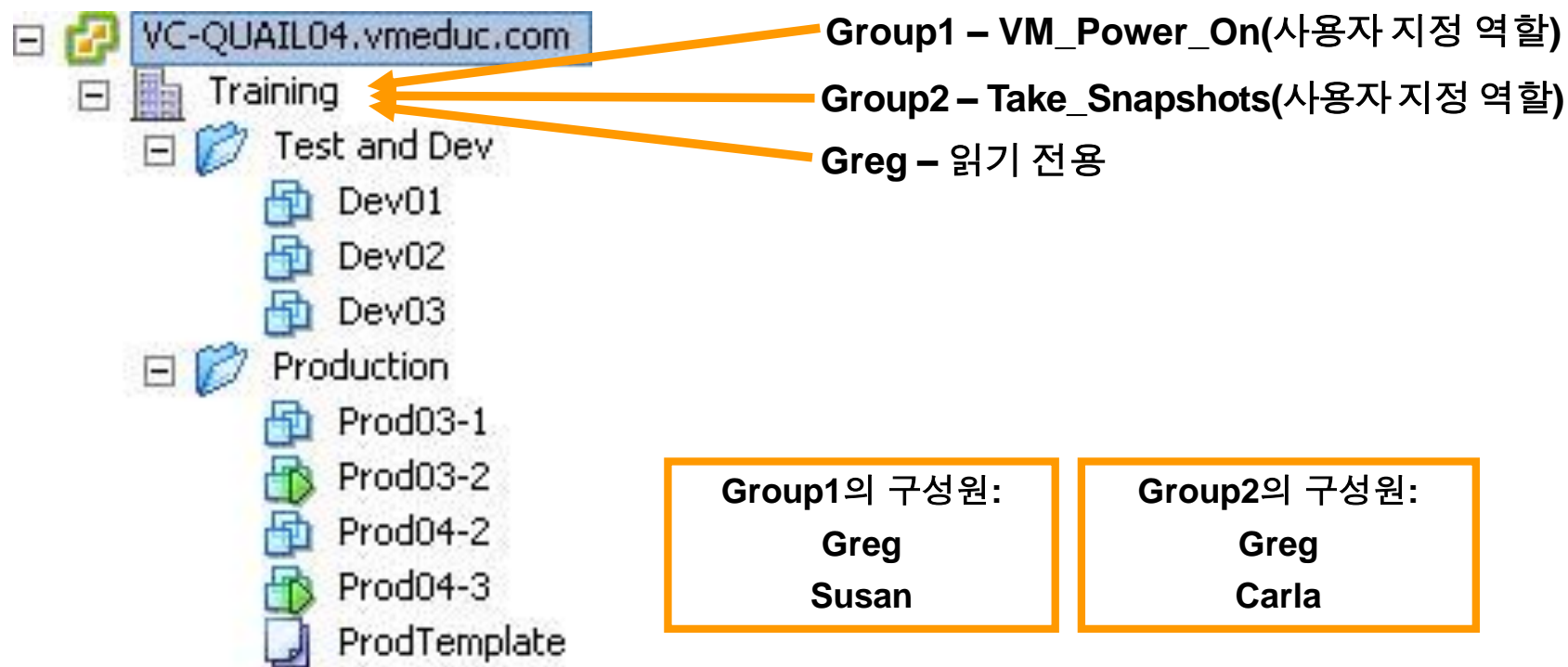
사용자가 여러 객체에 대한 사용 권한을 가진 여러 그룹의 구성원일 경우,

- 사용 권한을 가진 그룹의 각 객체에 대해 사용자에게 직접 부여된 것처럼 동일한 사용 권한이 적용됩니다.



사용 권한 적용 시나리오 4

객체의 사용자에게 명시적으로 정의된 사용 권한은 해당하는 동일한 객체의 전체 그룹 사용 권한보다 우선합니다.



역할 생성

필요한 작업만 사용하도록 설정하는 역할을 만듭니다.

- 예: Virtual Machine Creator
폴더를 사용하여 사용 권한 범위를 포함합니다.
- 예를 들어, 사용자 Nancy에
Virtual Machine Creator 역할을 할당하고 Finance 폴더에 적용합니다.

Virtual Machine Creator 역할

데이터스토어 > 공간 할당

네트워크 > 네트워크 할당

리소스 > 리소스 풀에 가상 머신 할당

가상 머신 > 인벤토리 > 새로 만들기

가상 머신 > 구성 > 새 디스크 추가

가상 머신 > 구성 > 디바이스 추가 또는 제거

실습 14

본 실습에서는 사용자 액세스 사용 권한을 관리합니다.

1. ESXi 호스트에 직접 로그인을 시도합니다.
2. 사용자에게 비관리자 액세스 권한을 부여합니다.
3. ESX Admins AD 그룹을 탐색합니다.

실습 15

본 실습에서는 사용자 지정 사용자 역할을 사용합니다.

1. vCenter Server에서 사용자 지정 역할을 생성합니다.
2. vCenter Server 인벤토리 객체에 사용 권한을 할당합니다.
3. 사용 권한 유용성을 확인합니다.