fineDoc Number:	EDCS-<XXXXX>
Last Revision Date:	December 17, 2010
Created by:	Louis Watta
Template Ver. Number:	EDCS-XXXX Rev X

CAE

Nexus 1000V 1.4
Port-Profile changes White Paper

TABLE OF CONTENTS

1 Introduction

The Cisco Nexus 1000V, is a Cisco developed server virtualization switching architecture for VMware ESX environments. The Nexus 1000V enables policy based virtual machine (VM) connectivity, mobility of security and network properties, and a non-disruptive operational model for both Server and Network administrators.

Offering a set of network features, management tools and diagnostic capabilities consistent with the customer's existing physical Cisco network infrastructure and enhanced for the virtual world, the Nexus 1000V allows customers to accelerate their adoption of VMs through the unification & simplification of the physical and virtual networks. The n1000v also secures & simplifies the deployment & movement of VM’s to increase service velocity while maintaining and enforcing security policy.

1.1 White Paper

The purpose of this white paper is to walk the user through some of the significant changes that have been made to port-profiles in the 1.4 release

1.2 Assumptions

The assumptions of this white paper are that the reader has

- Installed VMware VC 4.0U1/U2 or VC 4.1
- Installed Cisco Nexus 1000V 1.4 on an ESX VM in HA mode
- At least 1 ESX/ESXi 4.0U2/U1 or 4.1 boxes with VEM module already loaded
- Created a Nexus 1000V Distributed Virtual Switch (DVS) under vCenter
- Added the ESX boxes to the Nexus 1000V DVS

2 Port-Profile Updates

New in this release are some changes to Port Profiles.

Atomic Port-Profiles.

- When modifying a port-profile that is in use, if the modification is rejected by any port, the modification will be rejected on the port-profile. This means a Port-profile definition and inheritance on interface is always consistent.
- If you add a new interface that inherits a port profile, but rejects a portion of the port profile configuration, then it will reject all of port profile and remain in the shut state. In this case, you can recovert the interface using the **no shut** command

Interface Overrides

- For example “shut” is the default value for a port state. If the port-profile has “no shut” then the interface override can put the interface back in “shut” state
- There is a “default” command that will return control the port-profile

Interface Caching.

- When an interface goes offline (ESX host is powered off, or uplink port is removed) a cache is maintained to remember all the changes that happens on a port-profile so that when it comes online they can be applied.
- This cache is very large. About 2000 entries

Show run Hierarchy

Currently "show run" shows port-profiles in alphabetical order. In 1.4 port-profiles are shown in the proper hierarchy. This allows cut and paste of config from one VSM to another.

New max-ports command for veth port-profiles.

This feature allows you to restrict the maximum number of ports that can be assigned to the port-profile. When specified maximum number of ports is reached, no more ports can be assigned.

Assign a Netflow flow monitor to a Port-Profile.

Previously it was not possible to assign a Netflow Flow in a port-profile.

Restricting Port Profile Visibility.

Users and roles can be assigned to port-profiles. Using the User and Group commands, the Nexus 1000V admin can assign who can use the port-profile. There is a new port-profile-role command.

2.1 Restricting Port-Profile Visibility

Requirements:

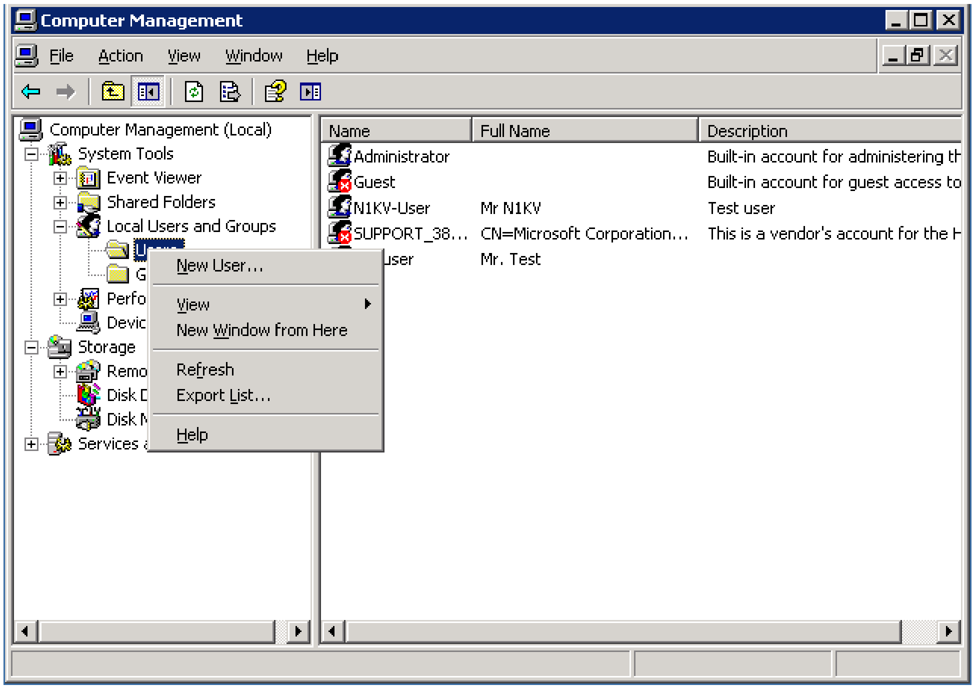
- Access to vCenter as Administrator
- Access to create a user locally on the vCenter Server
- Access to the VSM to create the port-profile-role

Create a User on vCenter Server:

If you already have a user other then Administrator you can skip this step. Otherwise create a simple local user on the Windows Server where vCenter is running.

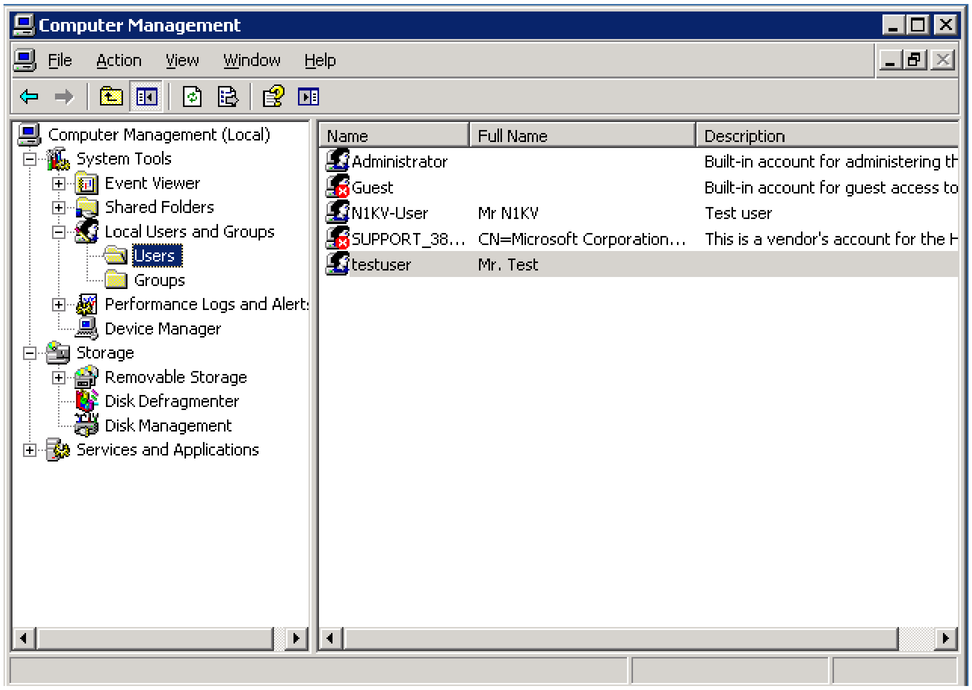
On the Windows server go to Start->Administrative Tools->Computer Management.

In the Computer Management application choose Local Users and Groups and then click on the Users Folder. Right click on the users folder and create a new user.



Name	Full Name	Description
Administrator		Built-in account for administering th
Guest		Built-in account for guest access to
N1KV-User	Mr N1KV	Test user
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account for the H
user	Mr. Test	

Create a new user and assign it a password. Here we created "testuser".



Name	Full Name	Description
Administrator		Built-in account for administering th
Guest		Built-in account for guest access to
N1KV-User	Mr N1KV	Test user
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account for the H
testuser	Mr. Test	

Next create the port-profile-role on the VSM.

```
n1000v-MV(config)# port-profile-role test-roles
n1000v-MV(config-port-prof-role)# user testuser

n1000v-MV# show port-profile-role
Name: test-roles
```

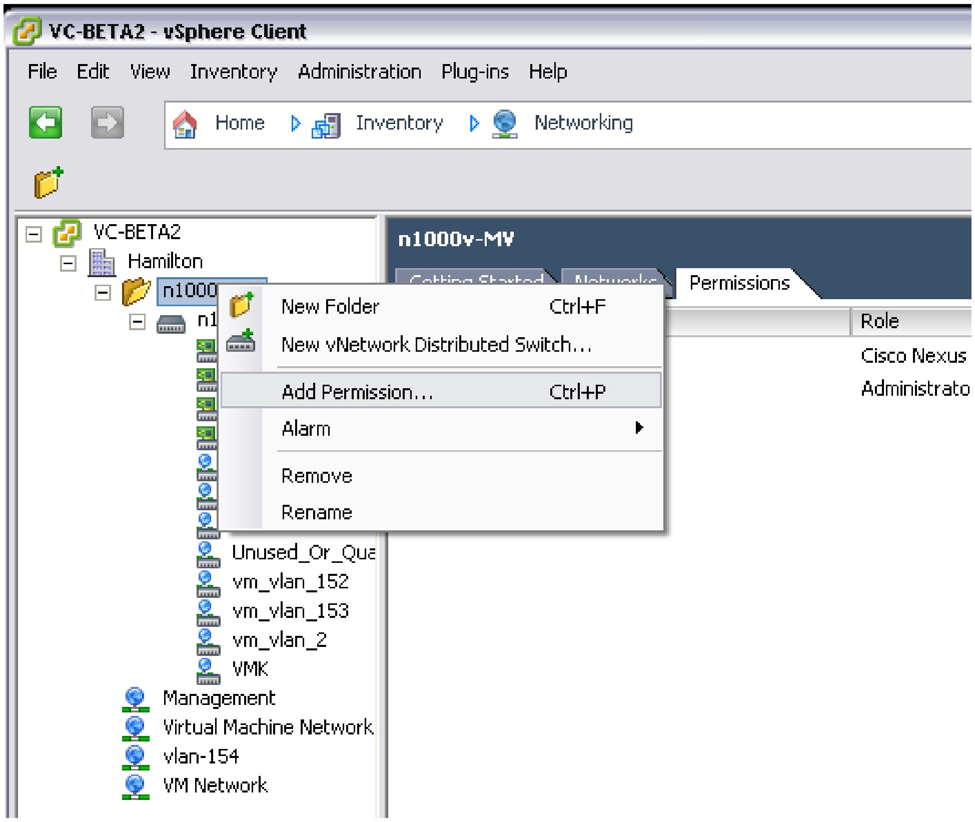
```
Description:
Users:
    testuser (user)
```

Assign the role to a port-profile. Here we will assign it to the vm_vlan_153 port-profile.

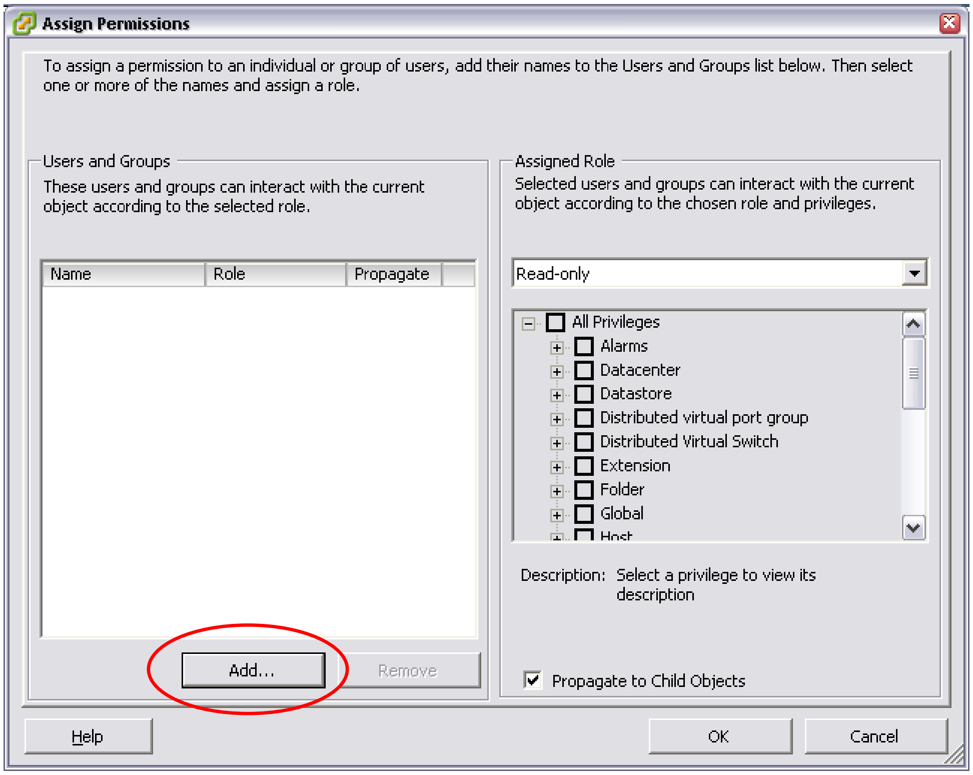
```
n1000v-MV(config)# port-profile type veth vm_vlan_153
n1000v-MV(config-port-prof)# port-profile-role test-roles

n1000v-MV# show run port-profile vm_vlan_153

!Command: show running-config port-profile vm_vlan_153
!Time: Wed Oct 27 15:22:57 2010

version 4.2(1)SV1(4)
port-profile type vethernet vm_vlan_153
  vmware port-group
  assign port-profile-role test-roles
  switchport mode access
  switchport access vlan 153
  switchport port-security
   no shutdown
  state enabled
```

Next assign the "testuser" access in vCenter. Log into vCenter as Administrator and grant "testuser" access to the following.

Click on Networking and grant access to the N1KV folder.



On the next screen click “add”



To assign a permission to an individual or group of users, add their names to the Users and Groups list below. Then select one or more of the names and assign a role.

These users and groups can interact with the current object according to the selected role.

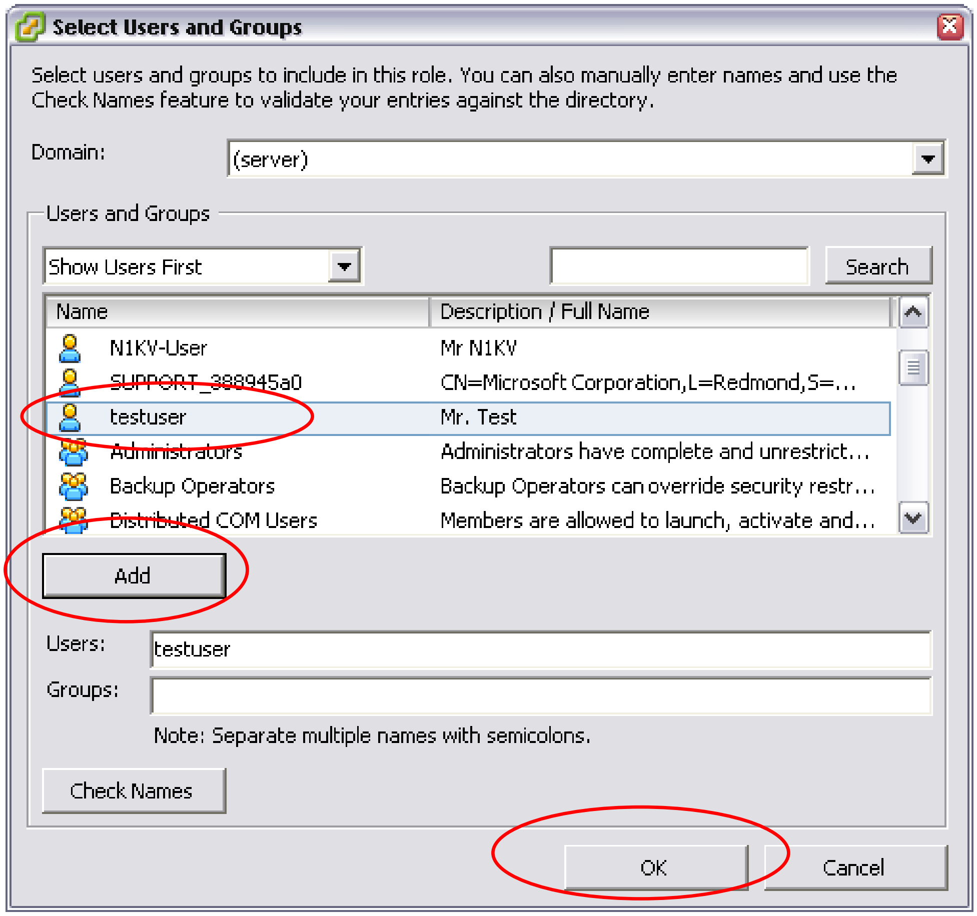
Selected users and groups can interact with the current object according to the chosen role and privileges.

Read-only

Description: Select a privilege to view its description

☑ Propagate to Child Objects

Find and Select testuser and then click add and then click OK.



Select Users and Groups

Select users and groups to include in this role. You can also manually enter names and use the Check Names feature to validate your entries against the directory.

Domain: (server)

Users and Groups

Show Users First

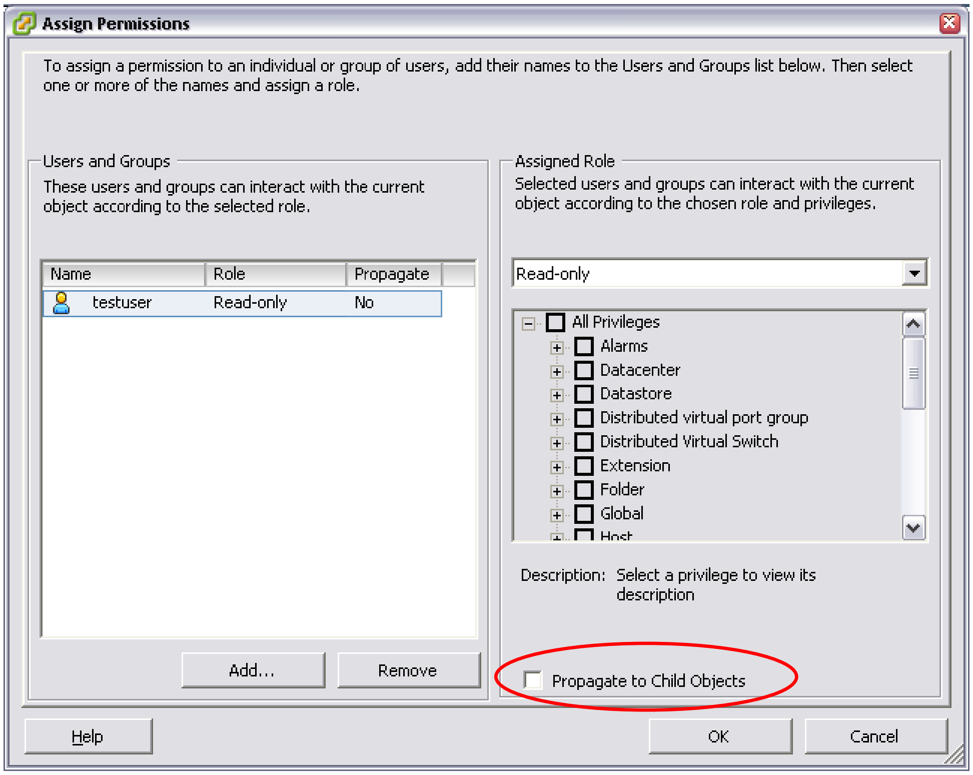
Name	Description / Full Name
N1KV-User	Mr N1KV
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=...
testuser	Mr. Test
Administrators	Administrators have complete and unrestrict...
Backup Operators	Backup Operators can override security restr...
Distributed COM Users	Members are allowed to launch, activate and...

Users: testuser

Groups:

Note: Separate multiple names with semicolons.

On the next screen make sure to unselect Propagate child objects and click ok



Assign Permissions

To assign a permission to an individual or group of users, add their names to the Users and Groups list below. Then select one or more of the names and assign a role.

Users and Groups

These users and groups can interact with the current object according to the selected role.

Name	Role	Propagate
testuser	Read-only	No

Assigned Role

Selected users and groups can interact with the current object according to the chosen role and privileges.

Read-only

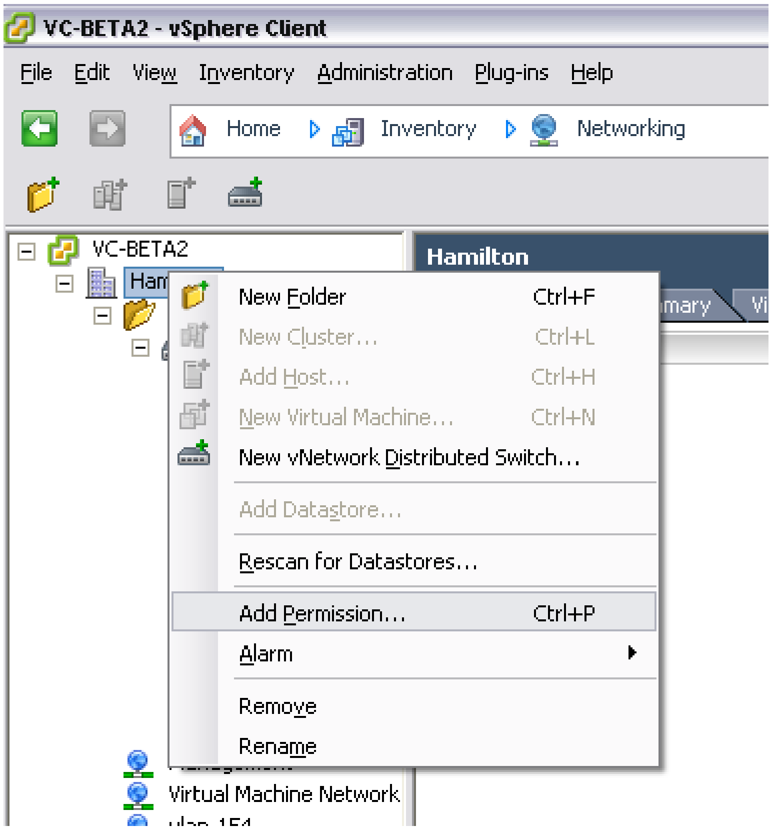
- □ All Privileges
  - □ Alarms
  - □ Datacenter
  - □ Datastore
  - □ Distributed virtual port group
  - □ Distributed Virtual Switch
  - □ Extension
  - □ Folder
  - □ Global
  - □ Host

Description: Select a privilege to view its description

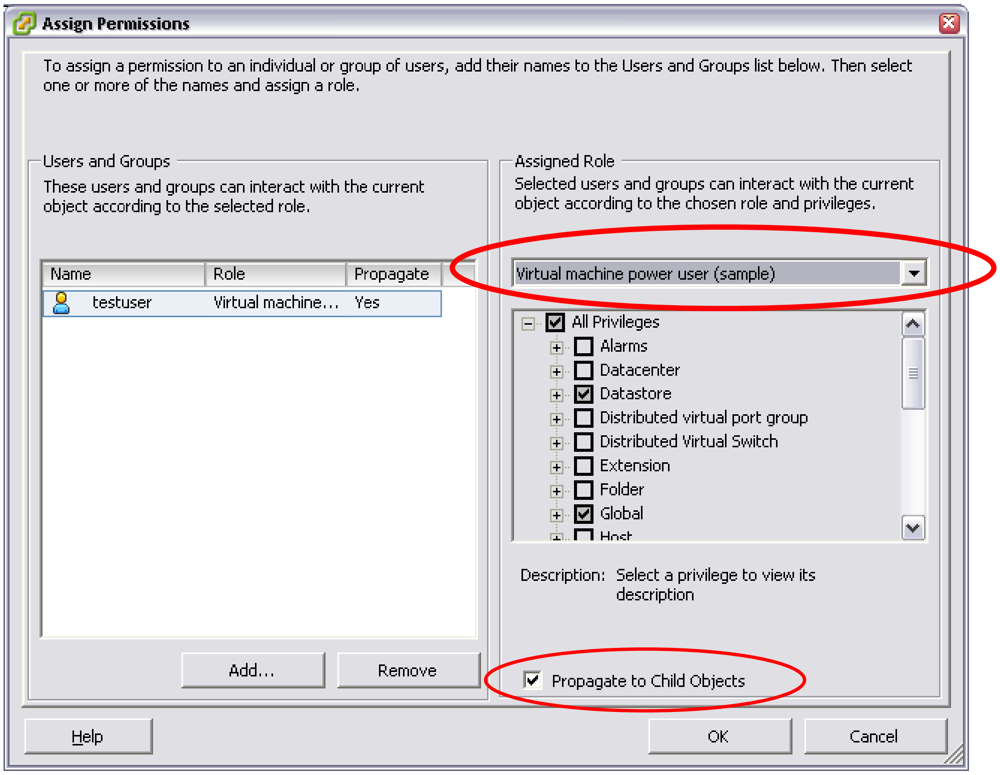
□ Propagate to Child Objects

Next we need to assign testuser basic privileges to access the VMs.

Click on the Datacenter where the VMs are and add privs just like you did above.



Again add testuser, but this time on the last screen choose Virtual Machine power user and leave propagate to child objects checked.


Assign Permissions

To assign a permission to an individual or group of users, add their names to the Users and Groups list below. Then select one or more of the names and assign a role.

Users and Groups

These users and groups can interact with the current object according to the selected role.

Name	Role	Propagate
testuser	Virtual machine...	Yes

Assigned Role

Selected users and groups can interact with the current object according to the chosen role and privileges.

Virtual machine power user (sample)

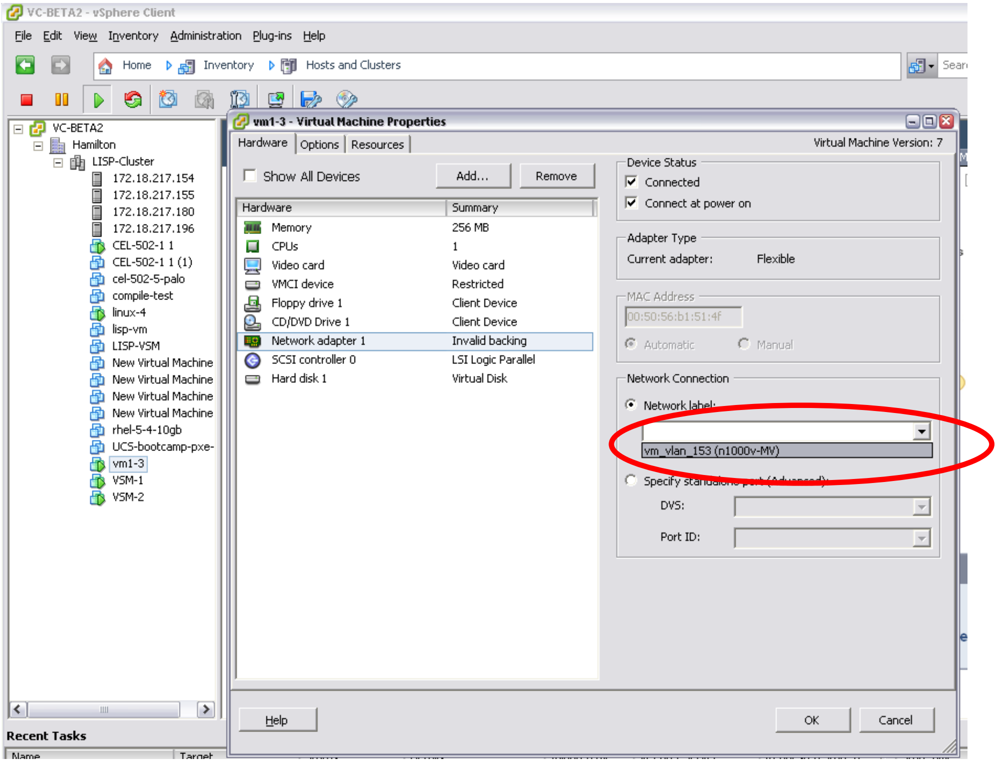
- ☑ All Privileges
  - □ Alarms
  - □ Datacenter
  - ☑ Datastore
  - □ Distributed virtual port group
  - □ Distributed Virtual Switch
  - □ Extension
  - □ Folder
  - ☑ Global
  - □ Host

Description: Select a privilege to view its description

☑ Propagate to Child Objects

Now login to vCenter as testuser, select a VM and try to modify the VM network settings.

The only networking option should vm_vlan_153



Hardware	Summary
Memory	256 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Floppy drive 1	Client Device
CD/DVD Drive 1	Client Device
Network adapter 1	Invalid backing
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk

Device Status

☑ Connected

☑ Connect at power on

Adapter Type

Current adapter: Flexible

MAC Address

00:50:56:b1:51:4f

● Automatic ○ Manual

Network Connection

● Network label:

vm_vlan_153 (n1000v-MV)

○ Specify standalone port (Advanced):

DVS:

Port ID: