VMware® Infrastructure 3

Advanced Technical Design Guide

~and~

Advanced Operations Guide

Two books in one!

Ron Oglesby
Scott Herold
Mike Laverick

Chapter 7: Access Control

You're probably quite familiar with the principles of allowing privileges from other systems you manage. If you are preparing for the Vi-3 exam you might want to spend some time making sure you are entirely happy with the difference between the built in roles used to assign privileges.

This chapter discusses the configuration of ESX and VirtualCenter for user rights. It is not unusual in large datacenters to have tiers of responsibility. Just as with ordinary users, we cannot depend on the good will of members of the IT department to stick within their job function. The only way to enforce change control is with tools that allow delegation.

Whether you use ESX in a stand-alone or with VirtualCenter the model for security is the same, the only difference being from where the users and groups come. With ESX in a stand-alone mode users and groups are created locally to the ESX host. If you use VirtualCenter your users and groups can be located in Active Directory, NT4 Domains, or users local to the VirtualCenter member server.

The model of security involves three components. Users or groups are added to VMware roles and these roles are assigned privileges. If you are a fan of the AGLP acronym you can think of VMware's model as GRP. Groups are added to roles, and roles are assigned privileges. In fact it's not possible in the GUI to bypass this method. It is impossible to assign to users or groups privileges without first using a role.

While we are on the subject of AGLP, I have found that VirtualCenter currently works in a very specific way with groups. The following approaches simply *do not* work:

- Using Global groups directly
- Using Global Groups added to Domain Local groups

What does work is the following:

- Users local to the VirtualCenter
- Groups to the VirtualCenter
- Domain Users in the Domain
- Accounts added to global groups, added to local groups on the VirtualCenter server

VirtualCenter would not duplicate the same privileges if you take the "hot standby" approach unless it is a duplicate of the primary. This can raise some interesting challenges.

As VirtualCenter has a system of folders, datacenter objects and sub-folders a system of inheritance does exist. So if you set role on a folder it will pass your privileges down the folder hierarchy. It is possible to stop this inheritance further down the hierarchy if you so wish. Of course, this system is not intended to be as sophisticated as file system's permissions system – but it is generally fit for its purpose. As with other systems you may have used, your position in the IT Management hierarchy has nothing to do with these hierarchies. So I might give a senior manager, who is not technical, read-only rights at the top of the tree – and give a Server Engineer administrator rights in a datacenter.

The Vi client does a very good job of hiding and disabling features for which the user has no privileges – so in the Inventory the user will find objects are hidden; ESX host names are not displayed; right-click menu options are greyed out and buttons on toolbars are disabled depending on your privileges.

In total, there are eight predefined roles. Three of these are available to a standalone ESX host and VirtualCenter, whereas the remaining 5 roles are only available to VirtualCenter. You can create your own custom roles with your own privileges. The eight predefined roles are as follows:

- No Access
- Read-Only
- Administrator
- Virtual Machine Administrator
- Datacenter Administrator

- Virtual Machine Power User
- Virtual Machine User
- Resource Pool Administrator

The first three (No Access, Read-only and Administrator) are common to both ESX and VirtualCenter. This book is not the place to discuss every single permissions difference between one role and another – clearly some roles such as "read-only" are self explanatory to anyone with experience of setting permissions and rights in other systems. But I would like to summarize the key differences. I recommend consulting VMware technical documentations for an exhaustive definition list of the privileges that make up a specific role.

No Access

This role is usually used for "exceptions to the rule." For example, say we have a group called "London" which contains 100 users, but 3 of those users should not have access to the resource in question. Rather than creating another group with 97 users, I add in the group – and then add in the 3 users (Bob, Harry, and Sue) and choose the "No Access" option. The effective permission for Bob, Harry, and Sue despite their group membership would be No access.

Administrator

This account has the highest privilege of all users. By default the Windows group of Administrators is the default group used with this role. This may not always be desirable – as a full administrator in Windows may not necessarily be a full administrator in VMware. There has to be default to allow access. In ESX 3.0.1 it is not possible to remove the last full administrator – however, in ESX 3.0.0 this was possible. ESX 3.0.1 fixed this "bug." By default, the root account on an ESX host is a member of the administrators group

Virtual Machine User

This role only assigns a privilege to VMs. Used on a datacenter with inheritance it would allow the user to power on, off, reset and suspend a VM. It would also allow the user to open a remote console on a VM. Frequently, Windows or Linux operators are given this privilege unless a more appropriate method can be used to deliver them to their environment. For example, it may be more

viable to allow telnet ssh access to Linux operators and RDP access to Windows operators.

Virtual Machine Power User

This type of user has the capacity to change some (but not all) of a VM's settings. It allows access to some "advanced" VM options such as creating and reverting snapshots.

Resource Pool Administrator

We have yet to cover resource pools – but put simply it is possible to create pools of CPU and RAM and allocate groups of VMs to the pool. It offers a quick and easy way to assign resources at a group level rather than modifying the settings of each and every VM. The system allows me to delegate management responsibility to the pool. Given the highly specific nature of this role, it is usually assigned to the resource pool object itself rather than elsewhere in the inventory.

Datacenter Administrator

This role allows the user to create new datacenter objects. However, the user has very limited rights to interact with the VM. Specifically, the datacenter role has no privileges to create remote console sessions.

Virtual Machine Administrator

This role allows full control over a VM's properties – right down to the permission to delete VMs from the ESX host and VirtualCenter. Given the name you might think that wherever you set this role that would be all the user could do, but you would be wrong. Depending on where in the hierarchy this role is set, it is possible for this role to add and remove ESX hosts from VirtualCenter.

Now that we have a correct understanding of the roles and what privileges they possess it is time to configure them. To carry out the next series of tasks you will need a collection of test users and some groups. Of course the possible permutations of privileges are infinite, and it is not my intention to show every

permutation, but to give you a feel for how it is both to assign and use roles within VirtualCenter and ESX. In my case I created a Windows group called "Vi3 Authors" and added two user Windows accounts – Scott and Ron.

In this demonstration I decide to allow "Vi-3 Authors" access to Mike's VMs within the Virtual Machine and Templates view.

1. **Right-click the folder in VirtualCenter** where you wish to apply your permission.
2. Choose **Add Permission**.
3. Under **Users and Groups**, click the **Add button**.
4. **Browse your system for your user group** and click **OK.**
5. Under **Assigned Role** select the role; in my case I selected Virtual Machine User.

   Note:

   In the same dialog we also have the option of deciding if these privileges "Propagate to Child Object." Disabling this option would apply the privileges to this folder only and not sub-folders.

Copying and Creating Custom Roles

One of the problems with the "Virtual Machine User" role option for me is the fact that this privilege also allows Ron and Scott to connect the VMs in my folder to removable devices such as CD-ROMs and floppy drives and modify connections to vSwitch port groups. I know that modifying these settings can cause warnings and errors with VMotion, and I would rather they did not have this privilege. I can easily duplicate the "Virtual Machine User" role and remove this privilege from the copy.

1. Click the **Admin button** on the toolbar.
2. Right-click **Virtual Machine User** from the list, and choose **Clone**.

3. **Rename the clone to a unique and meaningful name** such as "Custom Virtual Machine User – No Removable Devices."

4. **Right-click the custom role**, and choose **Edit Role**.

5. Expand the + signs, and **navigate to + All Privileges, + Virtual Machine, + Interaction**, and **remove the tick** next to **Device Connection**.

6. **Return to your original folder where the built-in privilege was set**, and **select the Permissions tab**.

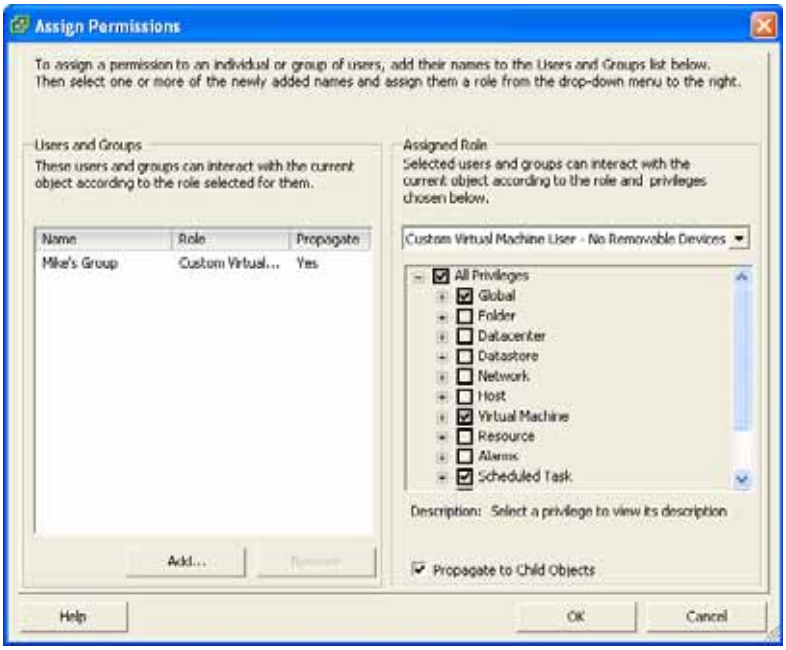
7. **Double-click the group** you assign the original role to, and select **Custom Virtual Machine User – No Removable Devices**.

   Note:

   Changes in privileges like this take immediate effect (as long as you use ESX 3.0.1 and VirtualCenter 2.0.1 or later) without the user being required to logout and login again. You should find that while users do not have right to *configure* the CD or floppy devices the privilege does not inhibit their rights to *connect* the CD or floppy devices.

Figure 7.1 shows me allocating my custom role to Mike's Group.

Figure 7.1



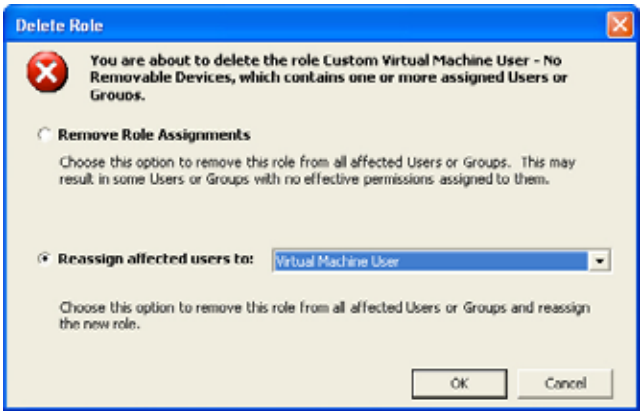
Removing Custom Roles

Removing a custom role is very easy; if you do it without first assigning an existing role to a user or group VirtualCenter will ask you to allocate another role first. This only happens if the role you are removing is currently in use somewhere in the VirtualCenter inventory. This is done to ensure that you don't deny your user rights altogether – crashing them out of the Vi Client through lack of any rights whatsoever.

Figure 7.2 shows the "Delete Role" dialog.

1. Click the **Admin button** on the toolbar.
2. Right-click custom role from the list and choose **Remove**.
3. Choose **OK**, to confirm you wish to delete it.
4. In the **Delete Role** dialog box select **Reassign affected users to**, and select an appropriate role.

Figure 7.2



VM Creation Rights

If you want to grant a user the right to create new VMs, a combination of privileges is required. Firstly, they need privilege of "Virtual Machine Administrator" in the folder hierarchy of Virtual Machines and Templates. Secondly, as you may remember from creating a new VM, you have to be able select an ESX host or DRS/HA cluster on which it will run. As a consequence groups and users will need "Virtual Machine Administrator" rights on either datacenters, individual ESX hosts, folders containing ESX hosts or DRS/HA clusters. The instructions below enable the ability to create VMs.

Allow Rights to a Folder in Virtual Machines and Templates

1. **Right-click** a folder in "Virtual Machines and Templates" where you wish to apply your permission.
2. Choose **Add Permission**.
3. Under "**Users and Groups**," click the **Add button**.
4. **Browse your system for your user group**, and click **OK**,
5. Under "**Assigned Role**" select the role. In my case I selected **Virtual Machine Administrator** for Mike's **Group**.

Allow Rights to Host & Clusters

1. **Right-click** in the "Hosts and Cluster" view one of the following: Datacenter, ESX Host, A Folder containing ESX hosts, A DRS/HA Cluster

   Note:

   In my case I select the "Intel Hosts" folder.

2. Choose **Add Permission**.

3. Under **Users and Groups**, click the **Add button**.

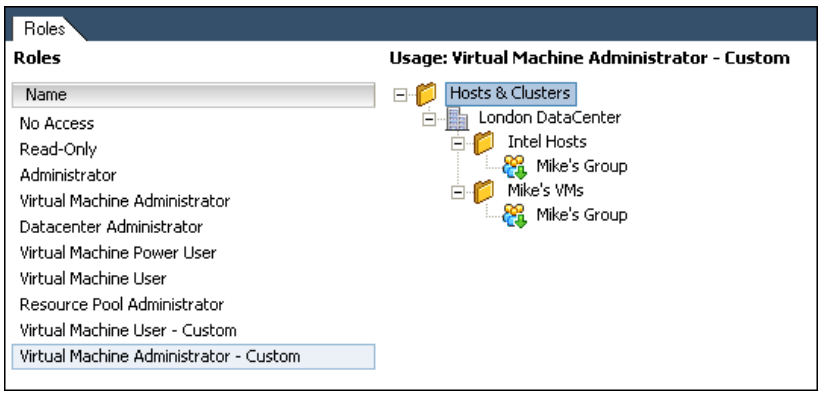
4. **Browse your system for your user group**, and click **OK**.

5. Under **Assigned Role** select the role. In my case I selected **Virtual Machine Administrator** and I choose **Mike's Group**.

   Note:

   Figure 7.3 shows how you can use Admin view to see where in the Inventory you have used your roles.

Figure 7.3



Using VMware Web-Access

On the ESX host and the VirtualCenter server there is web-service which runs. This is used to allow an "operator" style UI where operators can manage their VMs. The beauty of this service is that it only allows operators to manage VMs and nothing else, and it avoids the need to install the Vi-Client to every opera-

tor's PC. Web-Access requires no setup routine at all. All that is required is web-browser and the URL of the VirtualCenter or ESX hosts. If you point your web-browser at the VirtualCenter system, you will need to supply a Windows user account to login whereas if you point your web-browser at the ESX host, it will need local users created on it for it to work.

It has a number of neat features – firstly, the capacity for the operator to receive a console view of their VM and have this go into a full-screen view. Secondly, it has the ability to cut and paste a URL which points directly to the VM and to paste this to an email or a shortcut.

1. Open a web-browser to your VirtualCenter server, in my case this address.

   https://virtualcenter.vi3book.com/ui

   Note:

   Both ESX and VirtualCenter web-access generates a certificate using OpenSSL during the installation. The performance of web-access can be improved by either installing the built in certificate to your web-browser or creating a trusted certificate using your own Certificate Authority.

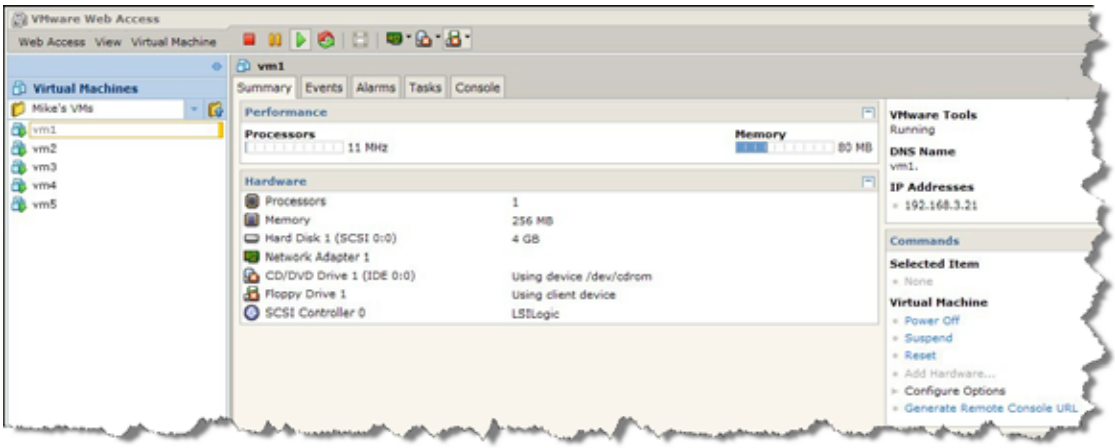
   Note:

   With Internet Explorer 7 you will have to allow pop-ups to this web-site.

2. Login with your VirtualCenter user name – I recommend testing this with a user account you have set up with limited permissions as it is more realistic.

   Figure 7.4 shows the standard layout of the web-access when managing a VM with the capacity to power on, off, suspend, and restart a VM on the toolbar. Additionally, we have the ability to manage devices such as the NIC, CD, and Floppy. The console tab will give you a view of your VM – it requires the install of an activeX control in Internet Explorer to work. Enabling the console view also enables the dimmed icon between the restart button and the NIC icon. This icon allows you to take the console view into a full screen (use [CTRL]+[ALT] to return to a normal view).

Figure 7.4



3. To generate a URL for a particular VM to be sent to use by email, under the Command Pane:

   Select Generate Remote Console URL.

4. Highlight the text in the light blue Generate URL box (like the sample shown below) and paste into an email.

   https://virtualcenter.vi3book.com/ui/vmDirect.do?view=d3NVcmw9aHR0cDovL2xvY2FsaG9zdDo4MDg1JnZtSWQ9VmlydHVhbE1hY2hpbmV8dm0tMjQ5JnVpPTM2_

Session Management

Now that we have multiple users connected via various privileges and interfaces it seems like a good time to mention session management. From the Vi Client it is possible to see who is logged on, disconnect Vi client users, and send a "Message of the Day." This message of the day is shown *every time* a Vi Client is connected and does not change until it is modified by the administrator.

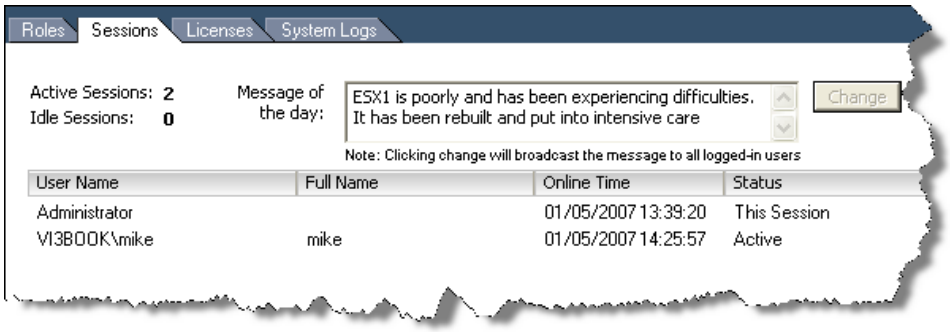
1. Select the **Admin** button on the toolbar.
2. Select the **Session** tab.

Figure 7.5 shows users Administrator and Mike are both logged on. The message of the day which I have input is displayed at every logon. As the note

states, modifying the text and clicking the change button transmits the messages to all sessions including your own.

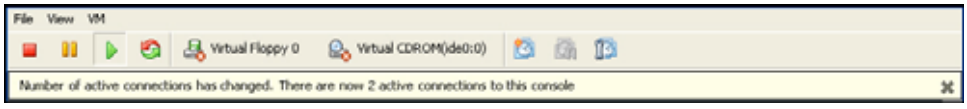
Right-clicking a user like VI3BOOK\Mike and choosing "Terminate Session" sends a message to the user and closes their Vi Client.

Figure 7.5



Session management also exposes itself when two users connect to the *same* VM using the VMware console. Figure 7.6 shows the alert that appears in the console title bar.

Figure 7.6



When this happens, it is possible for another user to interact with the VM at the same time as no attempt is made by VMware to "lock" the keyboard or mouse by the first user to open a console. In this respect a VM console is very much like an ILO/RAC or IP-KVM. This warning also appears if you open a console window and *also* open a console using the console tab available for each VM as shown in Figure 7.7.

Figure 7.7

Conclusion

In this chapter we have seen how it easy it is to delegate responsibility to others within your group or team. Web-Access is useful so long as your team only needs operator style access to VMs. It also stops you from having to unnecessarily install the Vi Client to lots of PCs.