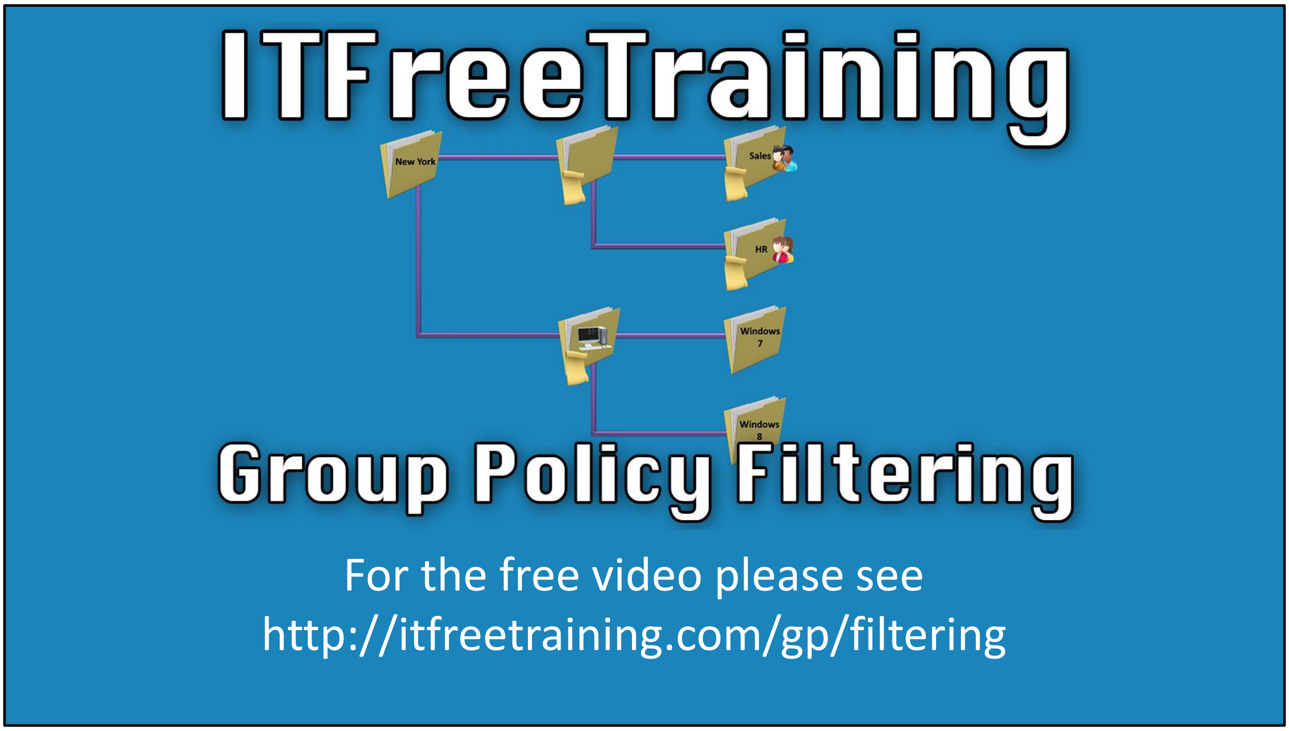
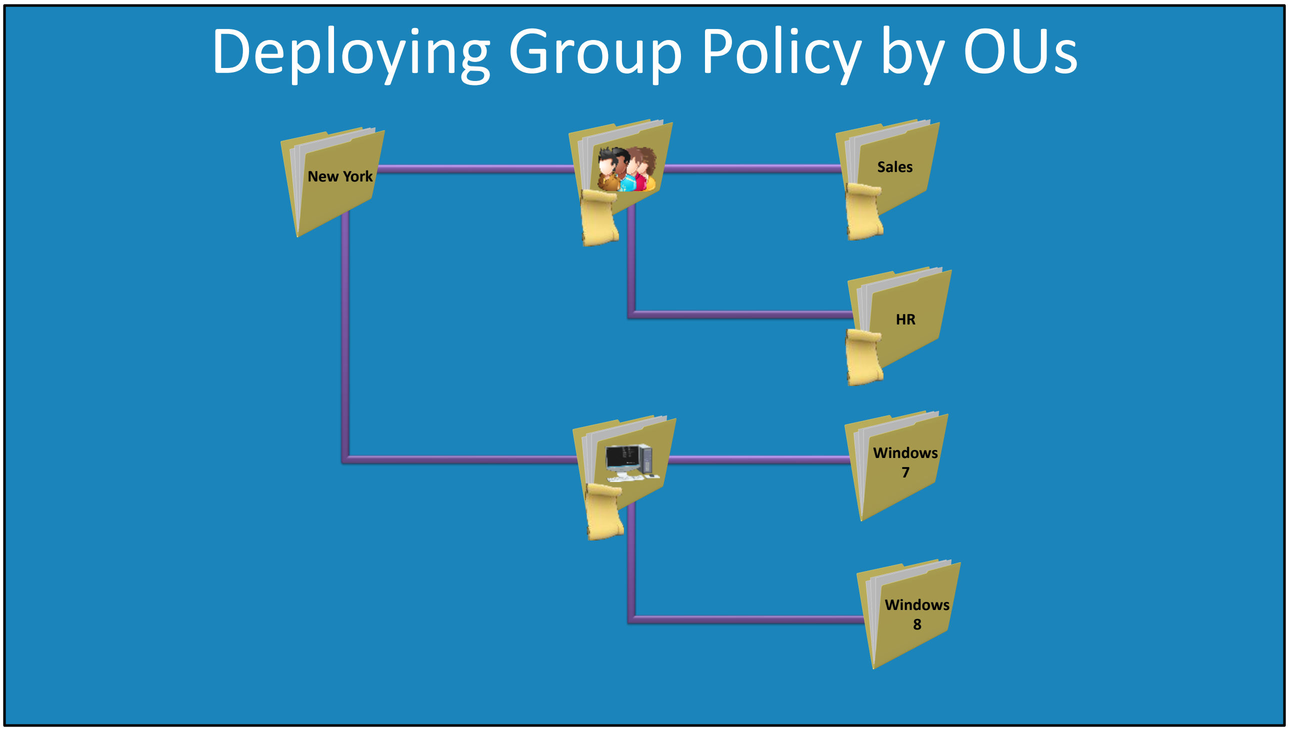


ITFreeTraining

Group Policy Filtering

For the free video please see
http://itfreetraining.com/gp/filtering

In this video from ITFreeTraining, we’ll review the process of utilizing filters within Group Policy via permissions. Group policy filtering provides an ability to target particular users and computers based on the administrator’s needs. This can significantly improve what an administrator can achieve and provides simplification of Group Policy management.



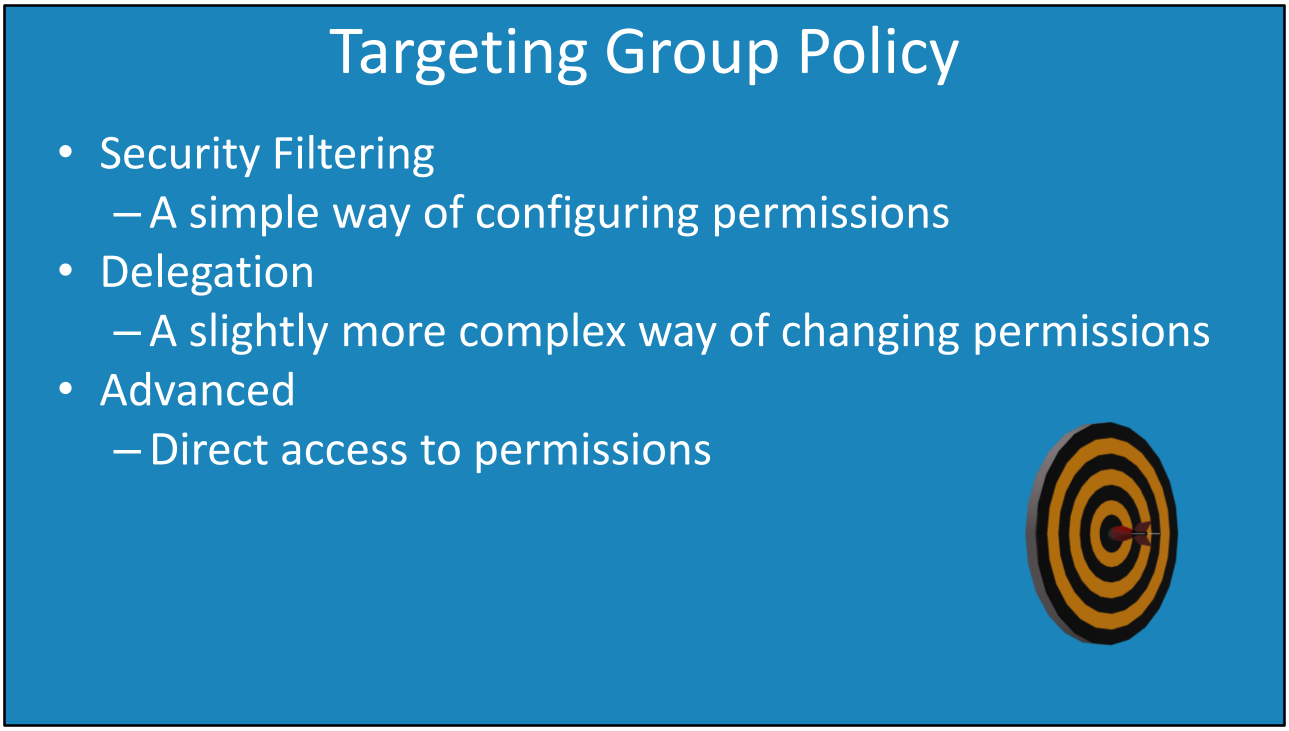
Deploying Group Policy by OUs

Deploying Group Policy by OUs

0:21 – An organization is free to configure their organization unit (OU) structure any way they like. Different geographical locations may be segregated into different OUs; in this example all users and computers located at the New York location may be put within the New York OU. The computers and users are created under an OU of New York. To allow Group Policy to target the specific OUs better, sub OUs are created for Users and Computers. This enables the ability to designate a separate Group Policy to be created that is for all users in New York and one for all the computers. Additionally, sub OUs can be made under the users. For example, individual departments such as Sales, HR or IT.

1:04 – With the OUs created, it is a trivial effort for an administrator to move users into the necessary OUs. Then all the administrator has to do is generate a Group Policy and apply it to those OUs. This could also be performed for the computers. Individual sub OUs could be created for Windows 7 and Windows 8 computers to deploy specific policies to different operating systems. This is useful for utilizing newer GP features that older versions may not support.

1:22 – Once again, the administrator has to ensure that they place the computer accounts in the appropriate OUs. This has the potential to create some issues such as in the case of computer upgrades. If a computer is upgraded from Windows 7 to Windows 8, the administrator would need to move the computer account after the upgrade. In small organizations, it can be much easier for an administrator to control and manage this aspect. However, as an organization gets larger, it becomes much more difficult to manage. Having a Group Policy system that can change automatically as needed can be very useful. The rest of our video will look at ways that an administrator is capable of achieving this.



Targeting Group Policy

- Security Filtering
  - A simple way of configuring permissions
- Delegation
  - A slightly more complex way of changing permissions
- Advanced
  - Direct access to permissions

Targeting Group Policy
1:55 – There are a variety of different methods to utilize targeting in Group Policy. The first way we will review is by utilizing Security Filtering. Security Filtering is basically a simple way of configuring permissions. It provides a way for an administrator to quickly change the permissions of a Group Policy object. The second method we'll take a look at is called Delegation, and is a slightly more complex method to change the permissions.
2:19 – The final security-related technique for Group Policy is the Advanced options. This is essentially direct access to the permissions of the Group Policy object. Each method leads to virtually the same result, but each technique has different advantages that should be considered. Let's take a deeper dive into the methods outlined above.

Demonstration

2:40 – First, we'll have to open Group Policy Management. Since we'll be altering the security of the Group Policy Object or GPO, we'll have to create a new GPO so this won't affect the other GPOs that have been implemented. To do this, we'll right click on the domain and then select "Create a GPO in this domain, and Link it here…"
3:02 – Put "Security Filtering" for the name of this GPO. Selecting the new GPO will present you with settings for "Security Filtering" at the bottom. By default, Security Filtering will have the group "Authenticated Users". This group contains all the authenticated users and computers within the domain. So essentially, this group contains any user or computer that has been authenticated by a Domain Controller.
3:29 – If I were to select the "Add" button, I am provided with the ability to add additional groups to this GPO's filtering groups. I'll go ahead and add the "Sales" group in our example. Upon adding the group, select it and then press the Properties button. The same information can be located in "Active Directory Users and Computers", however, this is more accessible if you are already in Group Policy Management. 3:48 – This is useful for instances in which you want to verify if individuals are members of a group. Cancelling out of this menu and looking back at Group Policy Management, you'll see that Authenticated Users is *still* present. Because of this, all the users that authenticate with a domain controller will be able to see and apply this policy.
4:10 – To ensure that the Group Policy *only* applies to the "Sales" user group, we'll have to select the "Authenticated Users" group and select the "Remove" button. Since "Authenticated Users" has been removed and the Sales group is known to only have users, no computer settings will be configured within this GPO. To capitalize on that, and to provide a quicker GPO deployment, we will select the "Details" tab and then under GPO status select the drop down menu to select "Computer configuration settings disabled". Configuring this will instruct GP to

only apply the user settings and any computer settings will be ignored. When creating a GPO that only has user or computer settings, it’s suggested that you disable the settings that are not relevant in order to speed up GPO processing.

5:00 – Once selected, I’ll be prompted to confirm that this is what I’d like to do. If at a later time, you add computer settings to this Group Policy, you could enable it again. Keep this in mind when you’re troubleshooting Group Policy. In the case that you need to add computer settings at a later time, you will need to re-enable these settings.

5:18 – The next tab we’ll review is the “Delegation” tab. This is where you can provide users with access to the Group Policy. This differs from Security Filtering because users added here will not be given the permission to apply this Group Policy. This tab’s essential purpose is in providing users with the ability to read, write, or delete Group Policy. When I say users, this would generally refer to other administrators or IT support staff, such as a helpdesk technicians. We’ll press the Add button and proceed to add the Marketing group. Notice that pressing the OK button will prompt you with what permissions to use. The available choices are read, edit settings, and lastly the option to give all permissions. In our case, we’ll enable the Read permissions and then select OK.

6:07 – You’ll notice that the Marketing group has now been added to the Group Policy and has the permissions configured to be able to read the GPO. Below this is the Sales Group with permissions that have been configured to read from Security Filtering. Users within the Sales group have the ability to apply the Group Policy and the users within the Marketing group will be prohibited from applying the Group Policy.

6:26 – To further understand what’s going on here, we’ll take a look by pressing the Advanced button. The advanced button will display the permissions for the Group Policy. If I were to select the Sales group, you should note that the permissions have been allocated below. These are “Read” and “Apply Group Policy”. In order for a user or computer to be able to apply Group Policy, both the “Read” and “Apply group policy” options must be checked. If I select the Marketing group, you’ll notice that the permissions “Apply Group Policy” is not checked and only the “Read” permissions is checked.

7:00 – The members of the marketing group will be able to read the Group Policy but will be unable to apply it. Closing out of this window, and selecting the “Scope” tab up at the top, you’ll notice that under “Security Filtering”, the Marketing group has been added. Any users, computers or groups that are added to permissions that have the “Read” or “Apply group policy” checked, will appear under “Security Filtering”. Here you can see that by adding users, computers or groups via the Add button is just an easier way to ensure that the proper permissions are checked.

7:34 – To demonstrate this better, we’ll select the ‘Delegation’ tab and then press the ‘Advanced’ button. With the permissions window open, we’ll highlight the group ‘Domain Admins’. You’ll see here that all the permissions are checked except for the permission ‘Apply Group Policy’. If we now check the permission ‘Apply Group policy’ and exit out of here to go back to the scope table, you’ll see that the ‘Domain Admins’ group now appears.

8:00 – So you can see here that Security Filtering and Delegation are both simple ways of configuring permissions. Security Filtering is designed with the intent of providing users, computers, or groups an ability to apply Group Policy. It’s aimed at providing administrators or those such as helpdesk staff or LAN Admins the ability to read and modify Group Policy as needed. Remember, when troubleshooting group policy, we only need two permissions in order to deploy Group Policy, which are ‘Read’ and ‘Apply group policy’.

Deploying Group Policy Using Security

Deploying Group Policy Using Security

8:30 – Now we'll review deploying Group Policy to users in your organization. Here we'll consider an organization unit (OU). In this OU, you place all your users. Now if you wanted to configure settings for the Sales users, you'll have to create a Group Policy and configure security for that Group Policy for the Sales user's group. Likewise, a second group policy can be created for the Marketing group. This means the administrator does not need to separate the users into specific OUs. Of course, the administrator will have to keep groups current but this is typically easier than separating users into separate OUs.

9:10 – The drawback to this method is that users or computers may have more than one Group Policy applied to them. For instance, putting users into OUs would mean the user would only receive one Group Policy. By using Security Filtering, you can see that two Group Policies are now being applied to the same user. One will be filtered out while the other will be applied. In a subsequent video, we'll review how to use Windows Management Instrumentation (WMI) to apply Group Policy.

9:35 – Using WMI, you can use computer characteristics, such as the operating system, in order to apply Group Policy. Until that video, thanks for watching and hope to see you in our other videos.

References

"Installing and Configuring Windows Server 2012 R2 Exam Ref 70-410" pages 321-322

Credits
Trainer: Austin Mason http://ITFreeTraining.com
Voice Talent: HP Lewis http://hplewis.com
Companion Document: Austin Mason http://ITFreeTraining.com
Video Production: Kevin Luttman http://www.KevinLuttman.com
Quality Assurance: Brett Batson http://www.pbb-proofreading.uk