Server-based Networking & Security

IS375 Group 5 Project

The purpose of this project is to put into practice what we learned in classroom.

Beatris M., Zim Y., Lawton P., Mike S.

12/13/2011

IS375 Group 5 Project

Document: Steps taken to complete project

Task 1: Initial assessment

Our domain is: **grp5is375.edu**

Role	FQDN	IP	Static IP?
Domain Controller	Grp5srv.grp5is375.edu	192.168.100.1	Yes
Server Core	MyServerCore.grp5is375.edu	192.168.100.20	Yes
Win7	Bea-PC.grp5is375.edu	169.254.163.130 (dynamic)	No

Static IP for Server Core: 192.168.100.2
CLI command:

netsh interface ip set address "local area connection" static 192.168.100.20 255.255.255.0 192.168.100.1

Task 2: Customize your Default Domain GPO

Default Domain policy "Grp5 Default Domain Policy"

2.1 Under computer configuration

Account policies:

Password policy Settings	Account lockout policy Settings
• Enforce password history: 5 • Maximum password age: 15 days • Minimum password age: 5 days. • Minimum password length: 7 • Passwords must meet complexity requirements: enabled	• Account lockout duration: an indefinite length of time • Account lockout threshold: 3 invalid logon attempts • Reset account lockout count after: 60 minute

Explain in your report the effects of the Account lockout policy setting:
The account lockout duration setting affects the user login to prevent unauthorized access to the domain and to ensure the user is valid. This set of policies will only allow each user three invalid attempts to log in. After three invalid attempts within 60 minutes, the user will be permanently locked out until the administrator resets the user's password. The counter that keeps track of invalid logon attempts resets after 60 minutes.

Other settings:
Security rights and options settings:
• Allow all Domain Users the right to be able to add workstations to your domain
• Enable "disconnect users when logon hours expire"

Explain in your report what each setting does:
-Allow all Domain Users the right to be able to add workstations to your domain

- This setting will allow all users within the grp5is375 group to add a computer to the domain.

-Enable “disconnect users when logon hours expire”

- With this policy is enabled, the user will be forcibly logged off when their logon hours expire.

Under /administrative templates/system/group policy:

• Change the group policy refresh interval for computers to 30 minutes with 20 minutes variations

• Change the group policy refresh interval for Domain controllers to 3 minutes with a 2 min variations

Explain in your report what each of the above settings does:

-Change the group policy refresh interval for computers to 30 minutes with 20 minutes variations

- Specifies how often Group Policy for computers is updated while the computer is in use (in the background). This policy specifies a background update rate only for Group Policies in the Computer Configuration folder.

-Change the group policy refresh interval for Domain controllers to 3 minutes with a 2 min variations

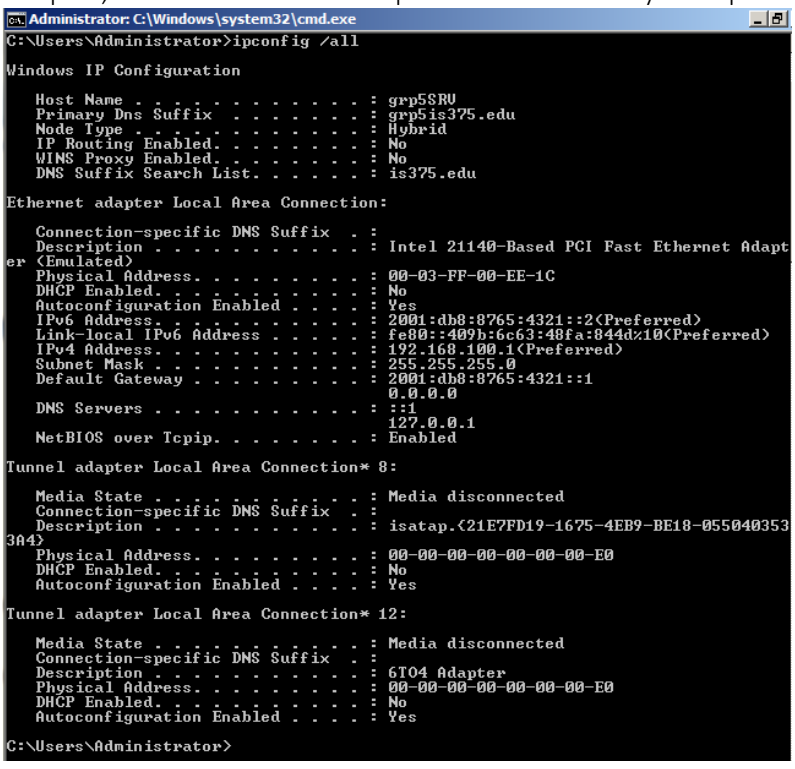
- Specifies how often Group Policy is updated on domain controllers while they are running (in the background). The updates specified by this policy occur in addition to updates performed when the system starts.

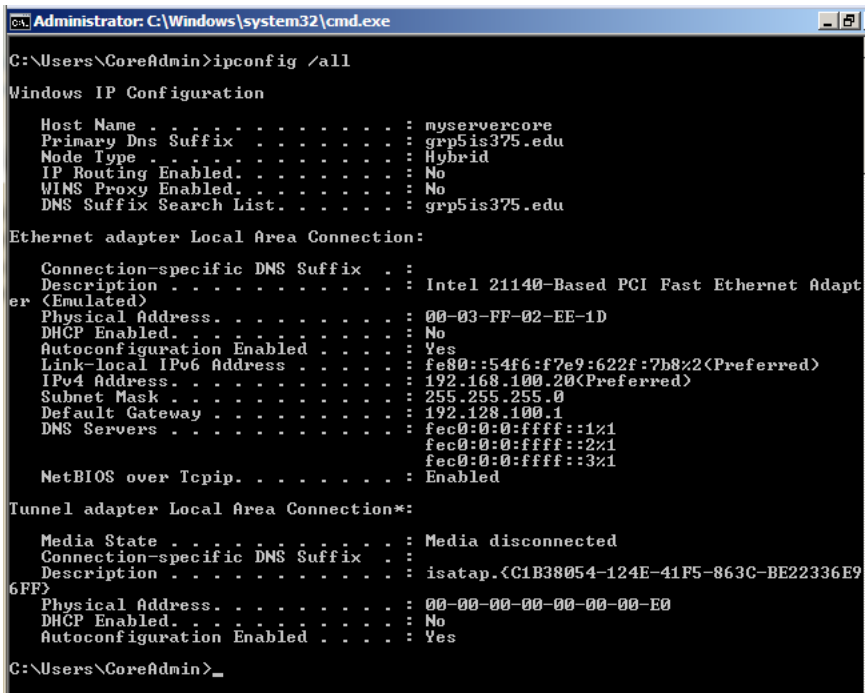
DNS Policy Settings:

• Refer to Fig. 6-13 on page 222, complete Activity 6-7.

• In step 7, enter the following DNS suffix names: is375.edu, isdept.is375.edu.

• Get screen shot at step 10, and a screen shot at step 13. Include both in your report





2.2 Under User configuration

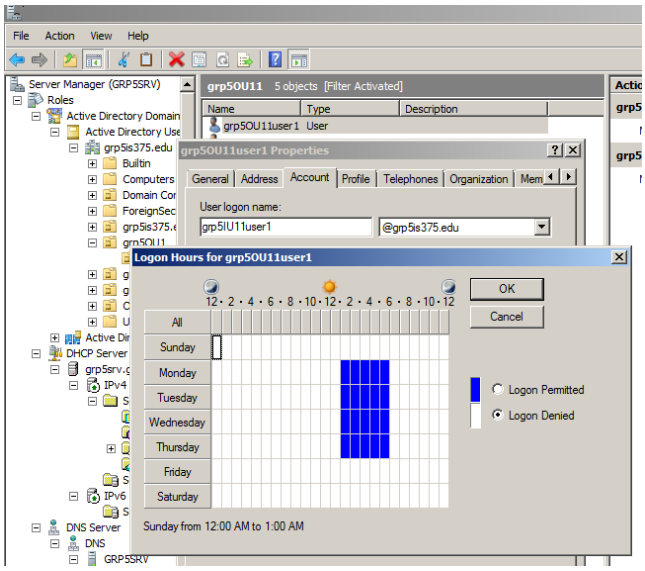
• Enable “Don’t run specified Windows applications” and disallow “notepad.exe” to be executed on client stations
• Enable “Prevent access to registry editing tools”
• Disable “Windows automatic update”
• Disable “Programs and Features” tool in the control panel
• Disable Help and Support menu in the Start menu

Task 3: Create an OU structure like the following for your virtual network.

First level: grp5OU1, grp5OU2, grp5OU3
Second level: grp5OU11 within grp5OU1
Populate each OU with at least 5 user accounts, using the naming format: grp5OU5User#

For all user accounts in Grp5OU3, request password to be changed at next logon.

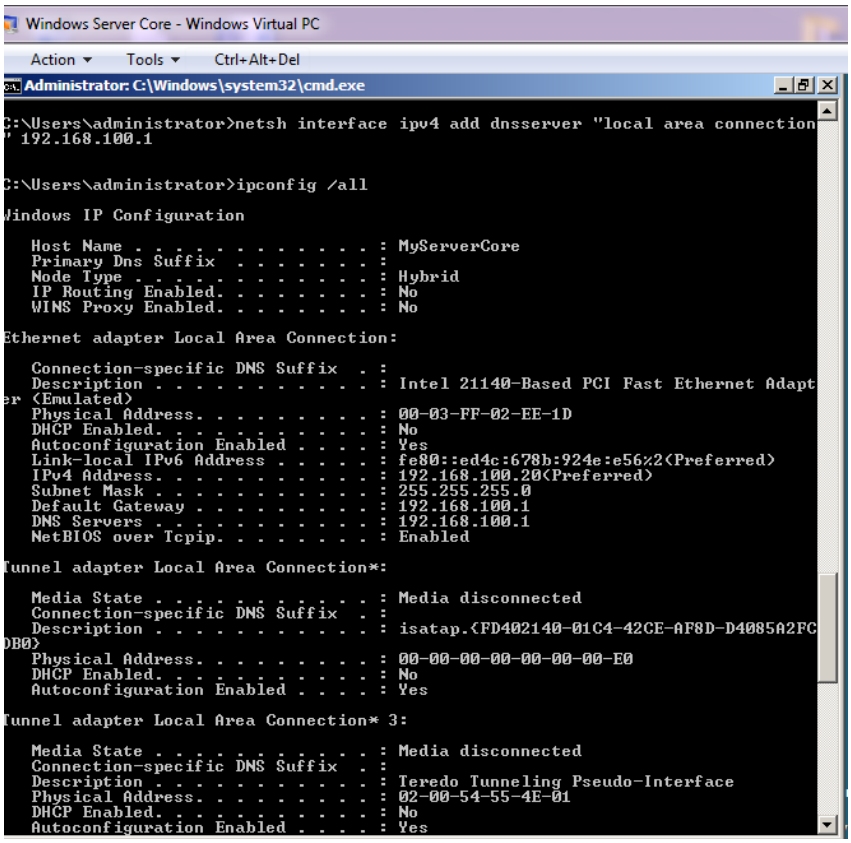
For all user accounts in Grp5OU2, enforce logon hours to be Monday through Friday from 8am to 5pm.
For all user accounts in Grp5OU11, enforce logon hours to be Monday through Thursday from 1pm to 6pm.



Task 4: Create a RODC on your server core VM (SCVM), while you full server 2008 DC VM (DCVM) is running. Follow the steps as described in Activity 6-20 on Page 251 of the text. Be sure to use your SCVM's name correctly.

1) Allow at least 5 minutes for your SCVM and DCVM to replicate the AD.
2) View AD users and computers on your SC, is it identical to primary DC (PDC)? Make a screen shot comparison and include them in your report.

-create dnsserver

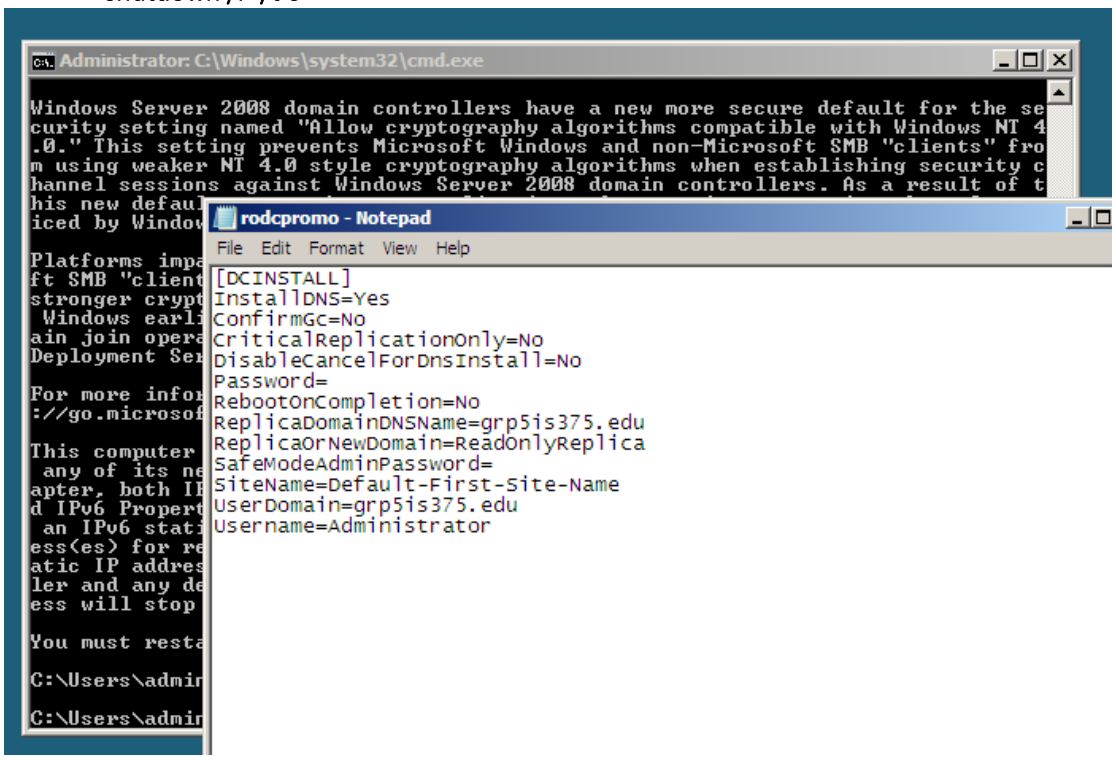


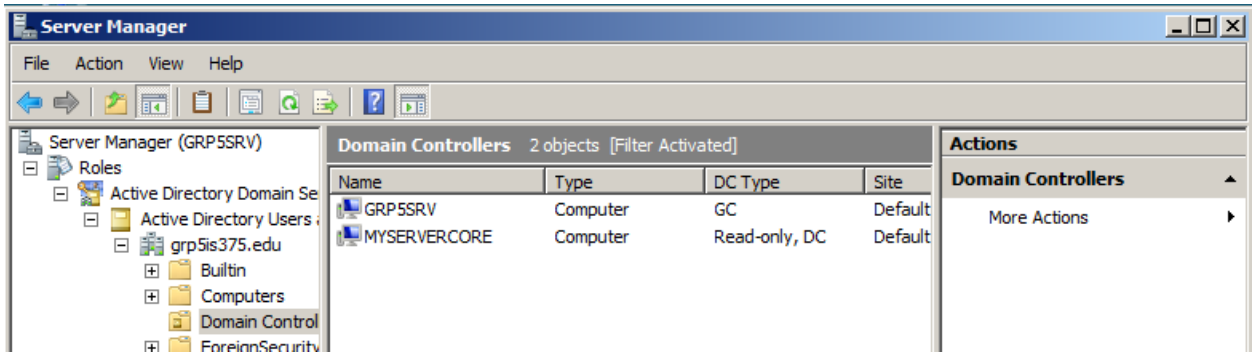
```
C:\Users\administrator>whoami
myservercore\administrator

C:\Users\administrator>netdom join \\myservercore /domain:grp5is375.edu /UserD:g
rp5is375.edu\administrator /PasswordD:P@ssword@
The computer needs to be restarted in order to complete the operation.

The command completed successfully.
```

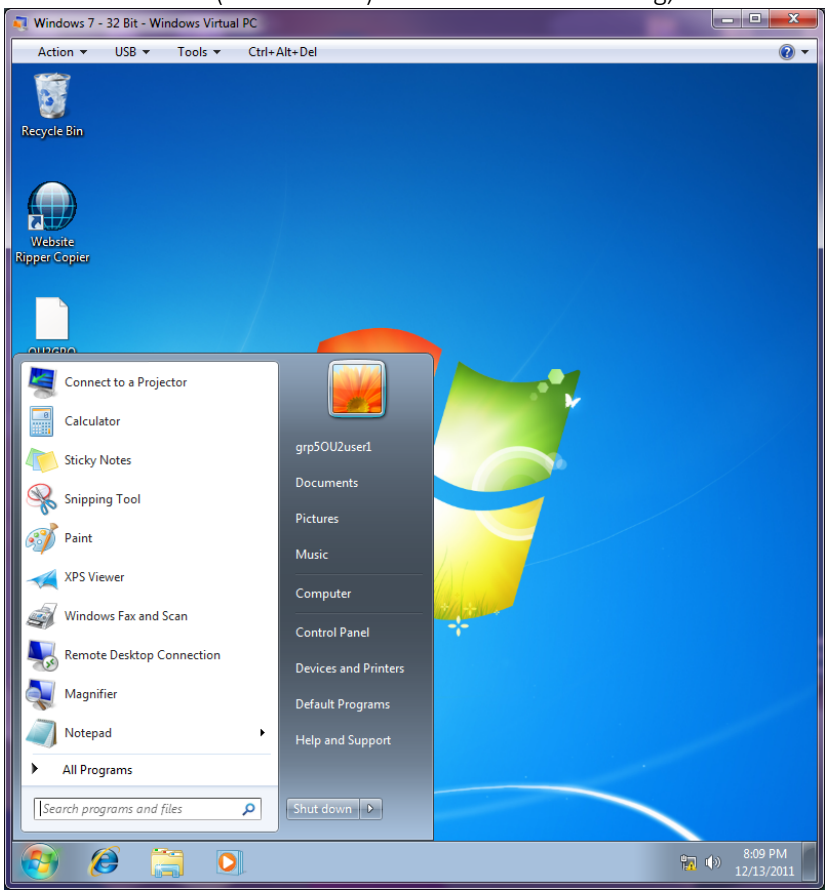
-shutdown /r /t 0





3) Turn off your PDC. Use a new domain user account to logon to your domain on Win 7. Can you logon? Explain. Capture a screen shot on Win 7 to show the result.

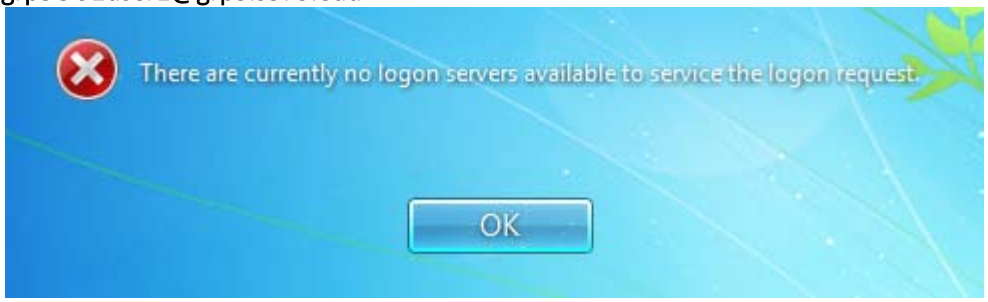
If we turn off PDC (Server 2008) and leave RODC running, we are able to log in Win7.



4) Turn off both your PDC and RODC. Use a new domain user account to logon to your domain on Win 7. Can you logon? Explain. Capture a screen shot on Win 7 to show the result.

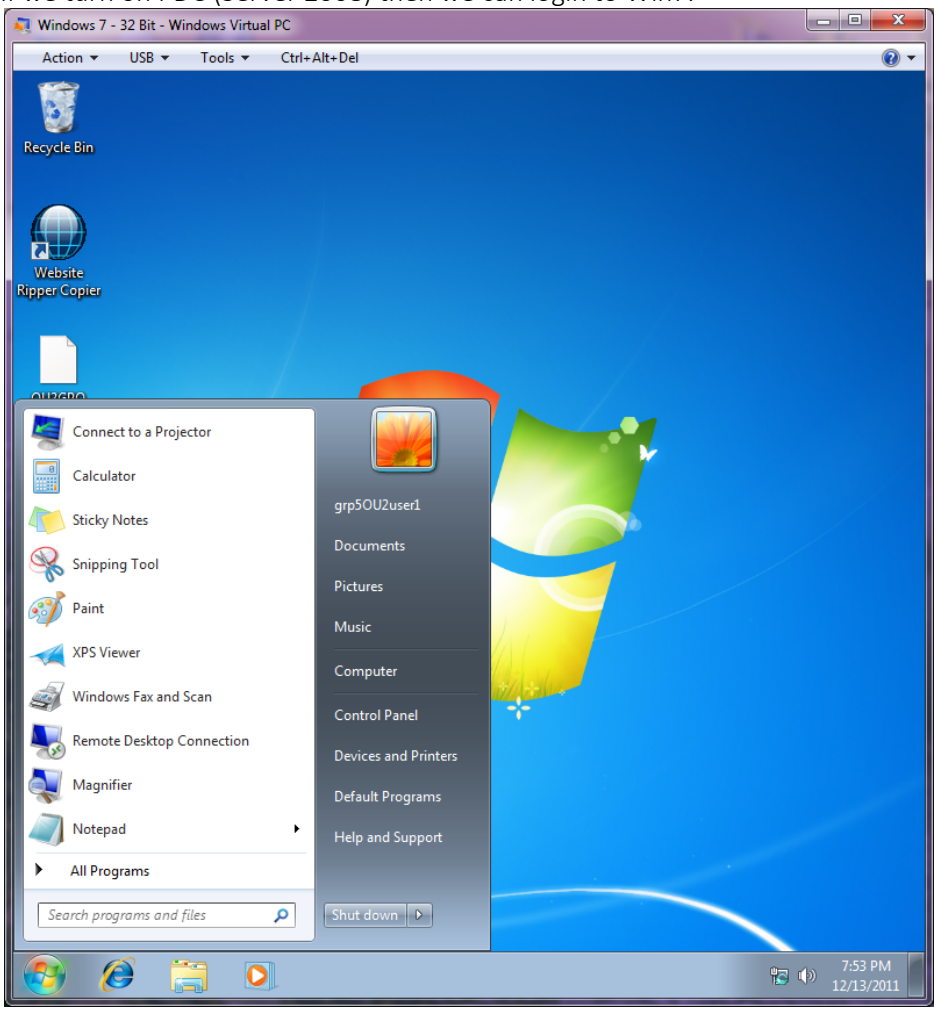
We cannot log on into Win7 because our PDC (Server 2008) and RODC (Server Core) are turned off.

grp5OU2user1@grp5is375.edu

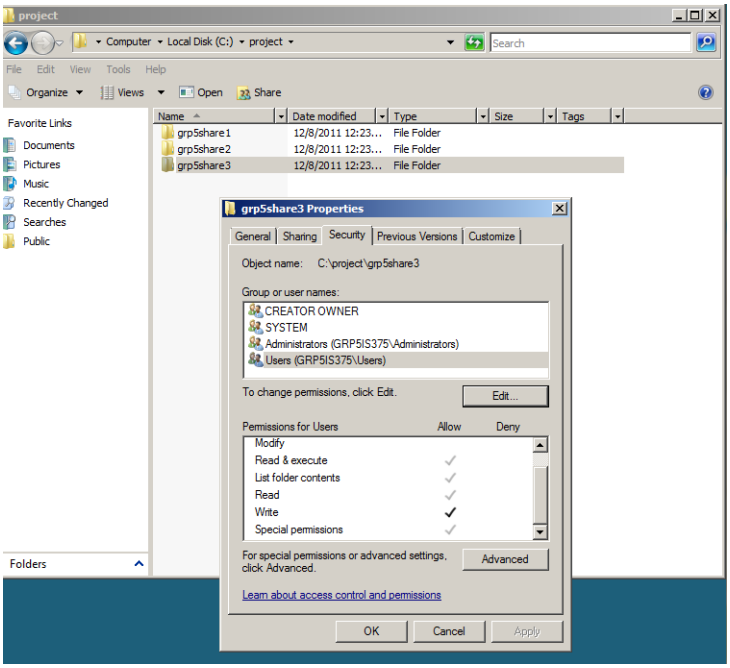


5) After 4) is completed, turn on your PDC.

If we turn on PDC (Server 2008) then we can login to Win7.



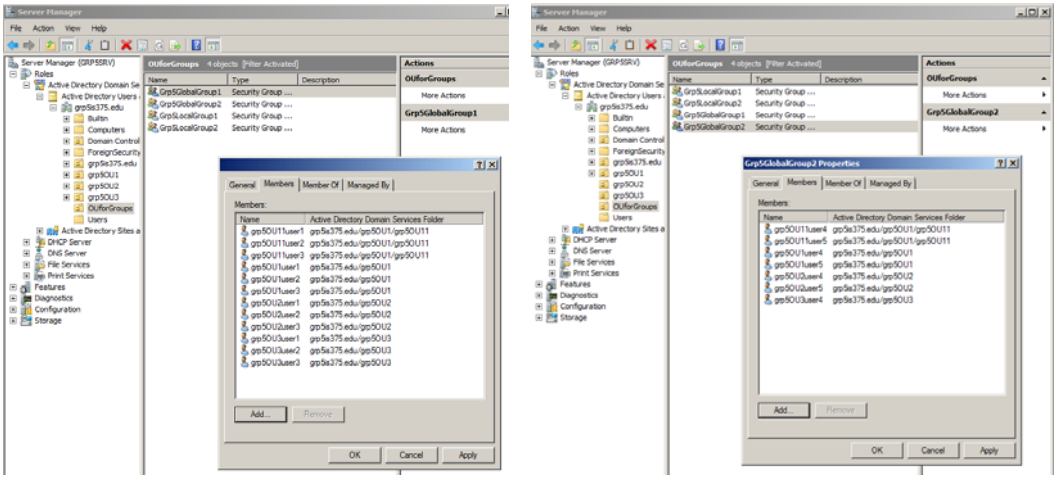
Task 5: Create 3 folders on your PDC, naming format: Grp5+share#
Populate each folder with several sample .txt files.
Make all domain users to have read and write permissions to access Grp#share3.



Task 6: Create the following security groups with the Naming format, and Create an OU called "OUforGroups" to contain the following groups created.

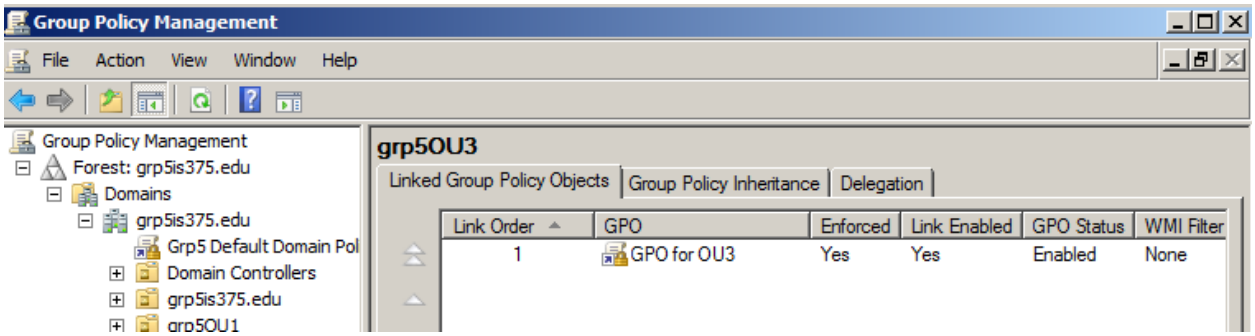
- Domain local groups: Grp5LocalGroup1, 2
- Global groups: Grp5GlobalGroup1, 2

Populate Grp5GlobalGroup1 with the first 3 user accounts from each OU.
Populate Grp5GlobalGroup2 with the last 2 user accounts from each OU.



Task 7: Create GPOs and Apply a GPO to an OU.

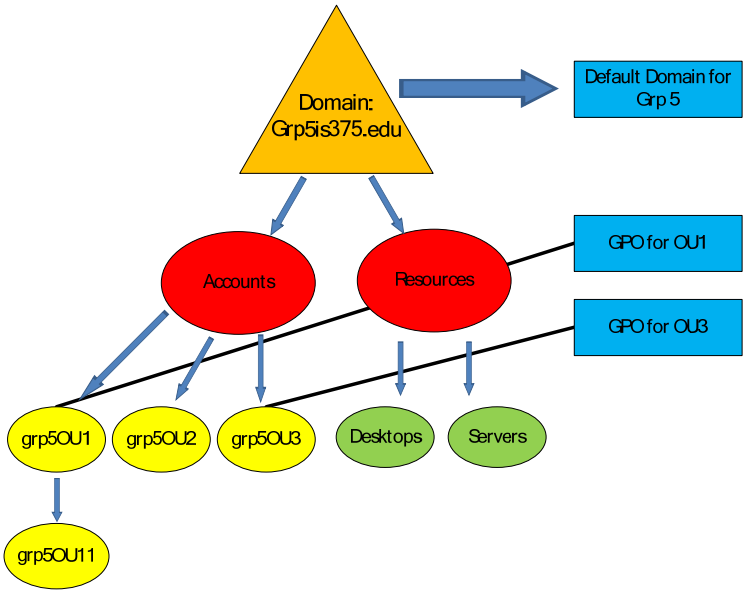
Create a “GPO for OU1”, and “GPO for OU3”. Link “GPO for OU1” to OU1; “GPO for OU3” to OU3.



Record in your report how you have completed this step.

To complete this step we went to "Group Policy Management," then we found the folders "Grp5OU1" and "Grp5OU3." On the folders we did a right click and selected "Create a GPO in this domain, and link it here..."; once it creates the GPO we rename it to “GPO for OU1” to OU1; “GPO for OU3” to OU3. Finally on the GPO Linked Group Policy Objects we did a right click and enforced them.

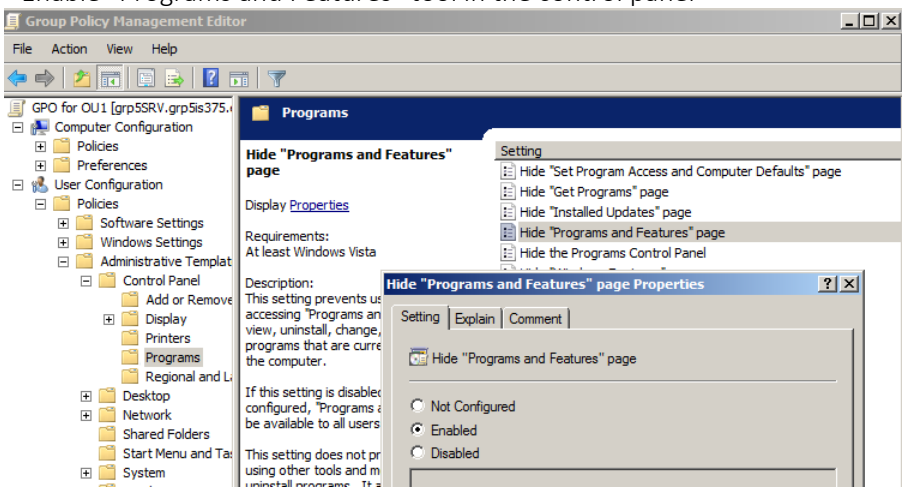
Draw a diagram and show how GPOs will be executed on each OU.



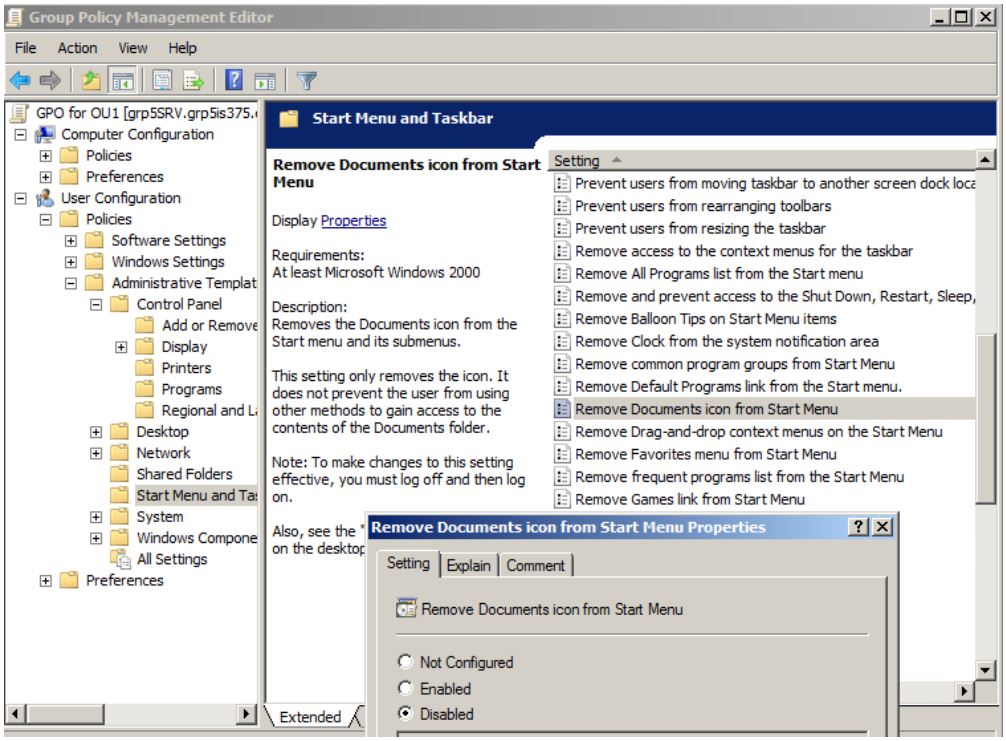
Task 8: Edit “GPO for OU1”

Use the following settings:

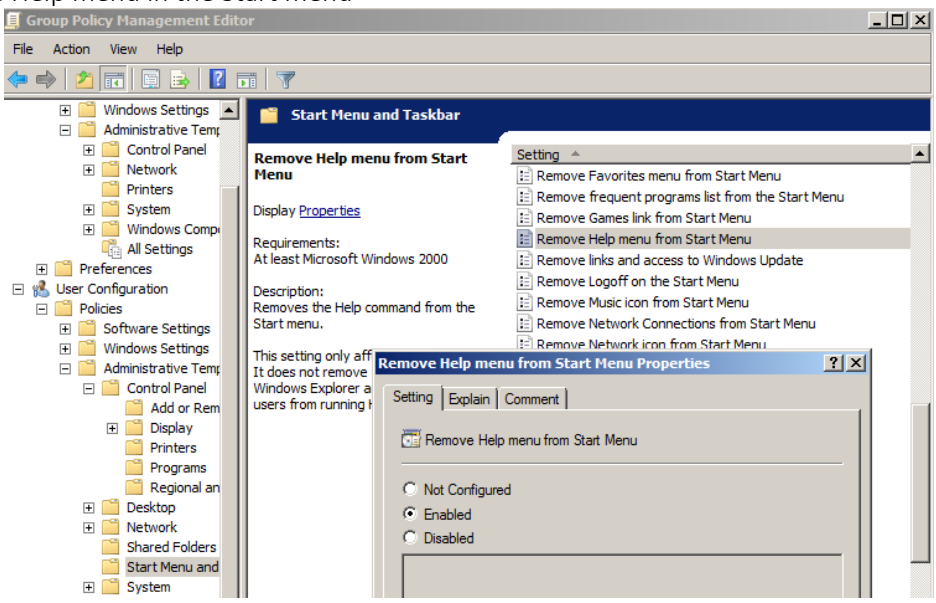
- Enable “Programs and Features” tool in the control panel



- Document menu is removed from the Windows Start menu

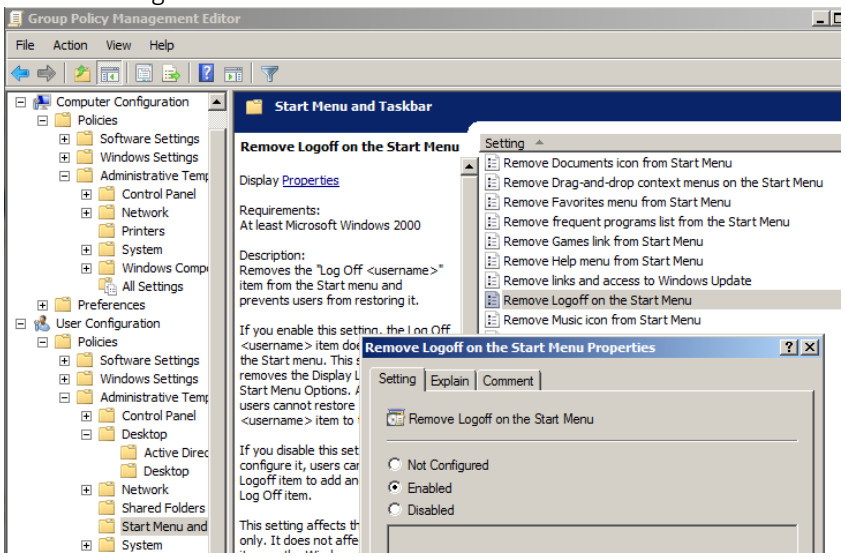


• Enable Help menu in the Start menu

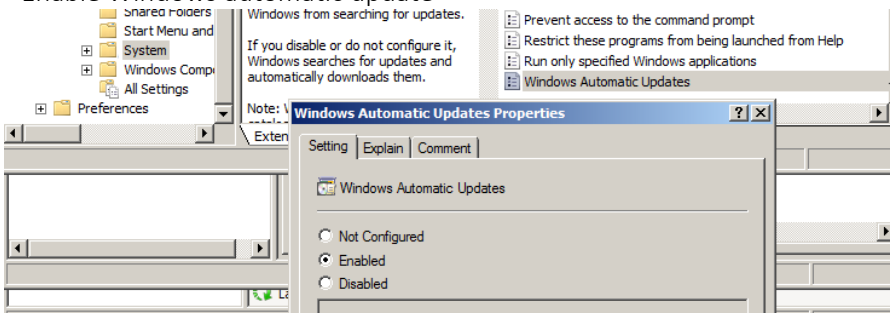


Desktop and start menu settings:

• Remove Logoff from the start menu

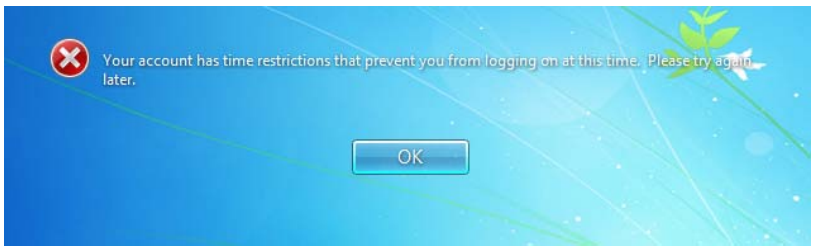


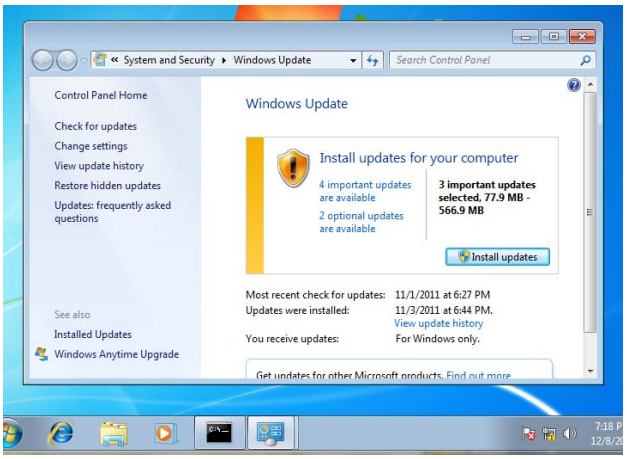
• Enable Windows automatic update



Use a user account in OU11 to test the GPO setting on Win 7. Compare with the default domain GPO, what are the effective settings implemented?

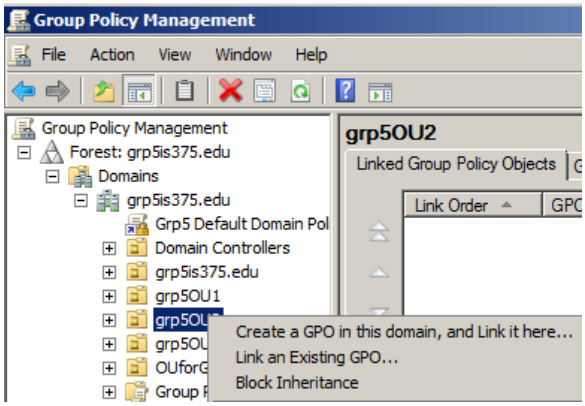
Compare with the default domain GPO, what are the effective settings implemented? Compared to the default domain GPO we can see program and features since we enabled it in the control panel. We cannot see any “documents” tab in the windows start menu. Help menu in the start menu is enabled. When you click on the start menu and try to log off you do not see a “log off” tab/option. Windows automatic update is enabled so an icon pops up stating automatic updates are ready to be installed.





Task 9: Enable “Block Policy Inheritances" on grp5OU2.

*grp5OU2 block inheritance and grp5 default domain policy not enforced



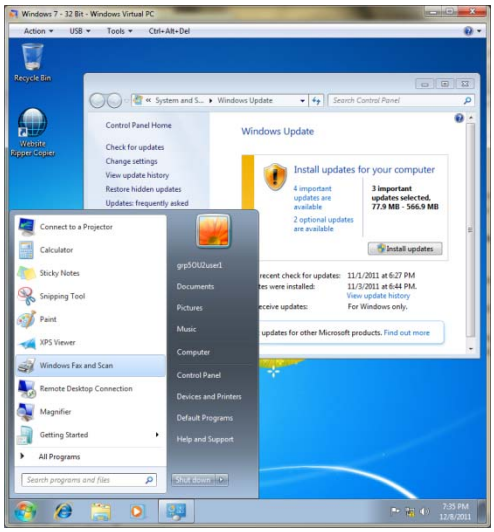
Explain what this means in your report.

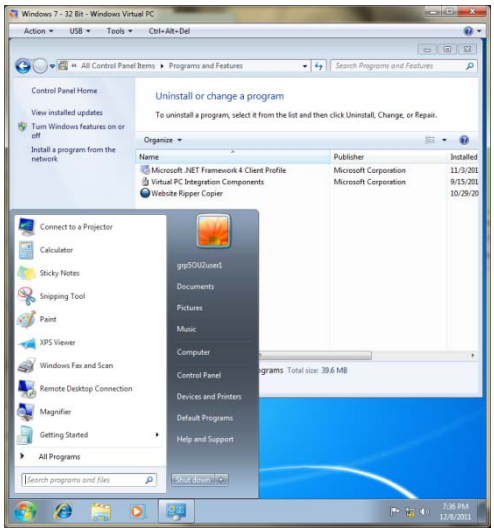
The Block Policy inheritance option blocks Group Policy objects that apply higher in the Active Directory hierarchy of domains, and organizational units. It doesn't block Group Policy objects if they have No Override enabled.

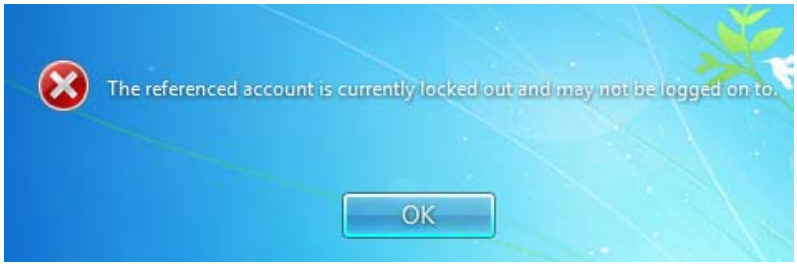
Use a user account in OU2 to test the GPO setting on Win 7.

Compare with the default domain GPO, what are the effective settings implemented?

By applying the Block Policy Inheritance on GPO for OU2 it should be the same as the Grp5 Default Domain Policy if enforced. If Grp5 Default Domain Policy is not enforced, the domain level GPO setting will not take effect on grp5OU2 as shown in the screen shots.

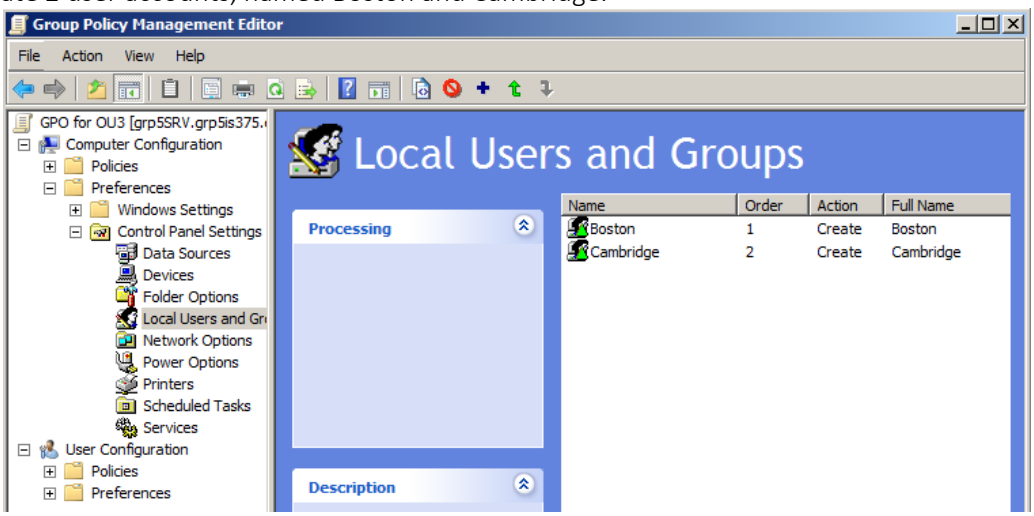






Task 10: Configure “GPO for OU3”

- Under the Computer Configuration/Preferences/Control Panel Settings/Local Users and Groups:
  - Create 2 user accounts, named Boston and Cambridge.

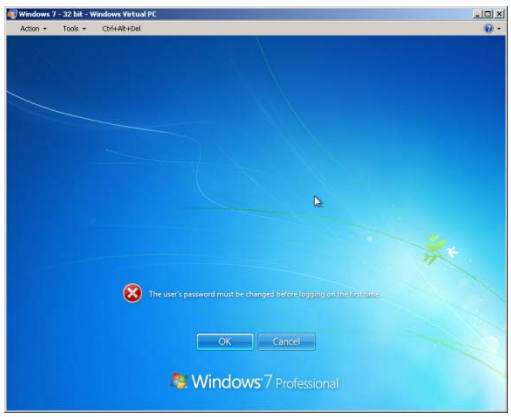


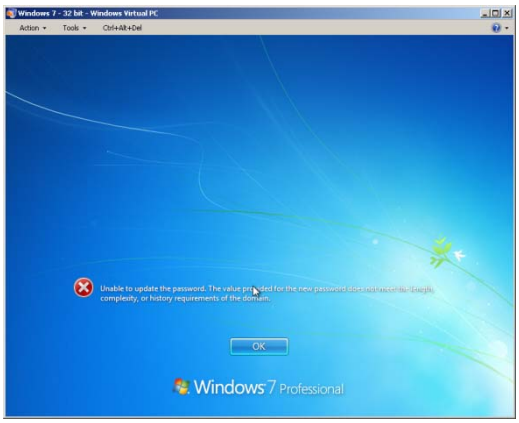
- Use the grp5OU3user5 user account in OU3 to test the GPO setting on Win 7.

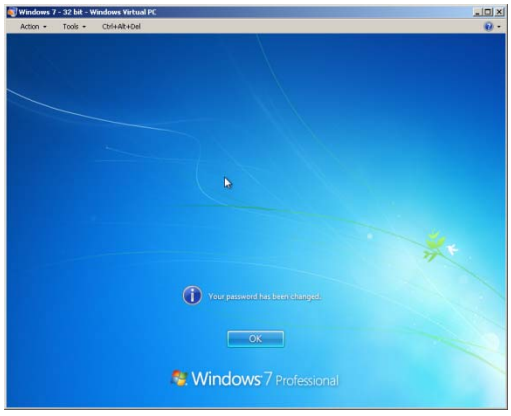
Compare with the default domain GPO, what are the effective settings implemented?

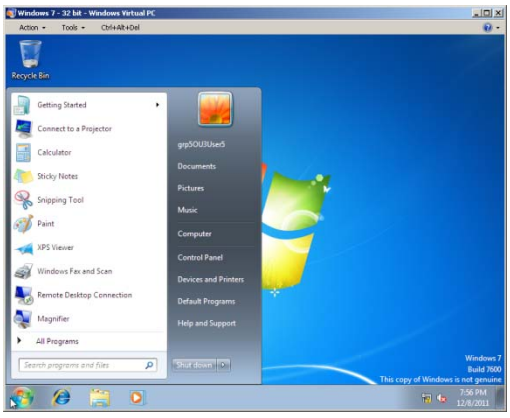
The effective settings implemented for grp5OU3user5 are the same as the Grp5 Default Domain Policy, except for first login, change the password.

- Verify and show the local user accounts on Win 7. Attach SS.









Task 11: Use security groups

- Make Grp5gloablgroup1 a member of Grp5localgroup1.
- Make your Grp5gloablgroup1 and Grp5gloablgroup2 members of Grp5localgroup2.

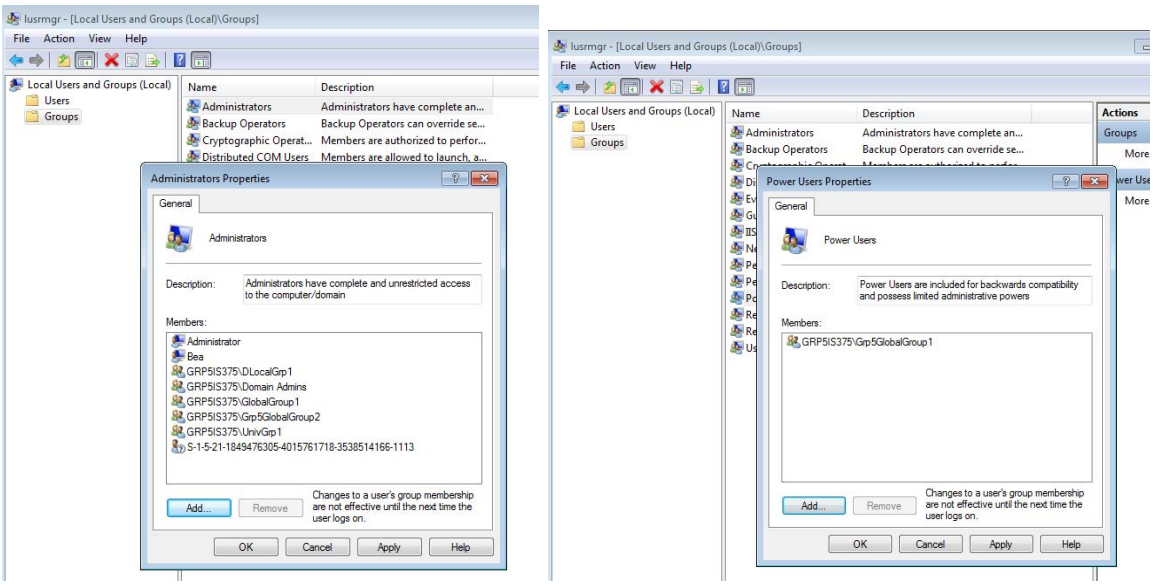
- In your report, explain the scenarios when use of domain local groups, universal or global groups is desirable.

-*Domain Local Group*: A security group that has the ability to contain universal, global, other domain local groups from all domains in the forest. These groups can be granted rights and permissions of resources on the same domain.

-*Global Group*: A group of users who can be granted rights and permissions, as well as, becoming members of other local groups. These users must be part of the global group's own domain.

-*Universal Group*: A security or distribution collection of users, other groups, and computers from any domain located within its forest. This group can be given universal security rights and permissions for resources within any domain in the forest.

- Logon to Win 7 VM as the local admin.
- Make the Grp5gloablgroup2 a member of the local Administrators group. And, make the Grp5gloablgroup1 a member of the local Power Users group.



Explain the purpose.

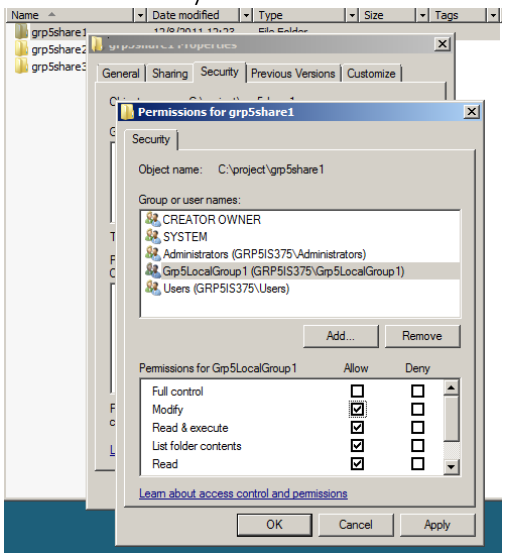
Local Administrator Group Permissions: A local administrator is different from a domain administrator. When authorized as a local administrator, you have administrative powers over the machine you are working with. The authorized user has the ability to view all files and run and install programs on the workstation. But if the user wanted to change domain wide settings they would need to log in using the proper credentials.

Local Power User Permissions: Allows users to run legacy programs and change COM object registrations, file associations, the Start menu, and install drivers for hardware devices.

Task 12: Control Resource Access

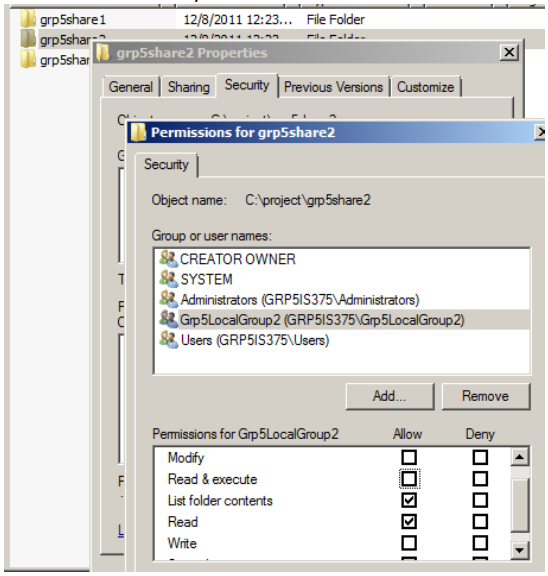
• Add Grp5localgroup1 to the ACL of Grp5share1. Give all permissions except Full Control. Also give all share permissions.

• Don't allow any other users to access this share.



• Add Grp5localgroup2 to the ACL of Grp5share2. Give only read and list folder contents permissions. Give only read share permission.

• Don't allow any other users to access this share.



• Can a group policy be assigned to a domain local group? What about a Global group?

- Yes, Group policy can be configured to affect all users on a computer or all users within a domain. If the domain local or global group exists within the same domain, then their permissions to control network resources can be restricted by the group policy.

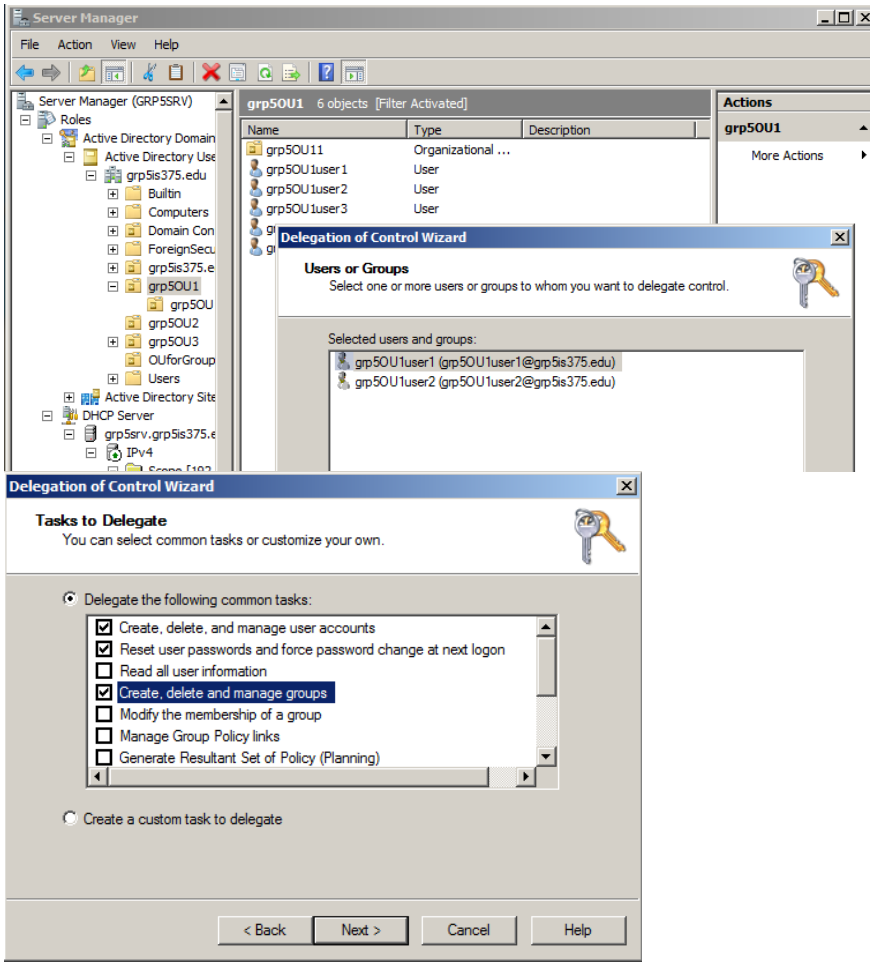
• What is the Full Control mean in the folder permissions?

- Granting a user full control in the folder permissions allows them to read, write, change, and delete files and subfolders

Task 13: Task: Delegate the Administrative Responsibilities

• For each OU, delegate the following administrative responsibility to the first two users (Grp5OU& user1 & Grp5OU user2):

- Create, delete and manage users accounts
- Reset passwords on all user accounts
- Create, delete and manage groups



• Record your steps in completing this task in your project report.

1. Go to Server Manager,
2. Find your OU folder,
3. Right click in the folder and select Delegate Control,
4. Add the users you want to delegate responsibilities,
5. Click Next,
6. Select the tasks,
7. Click Finish.

Task 14: Create Roaming Profiles

• Create a roaming profile for each of the 5 users in OU3. You may create a folder named C:|Profiles and given write/modify to domain users. Under this folder, each user will have a separate folder to contain the profile files.

• Record your steps of completing this task in your report.

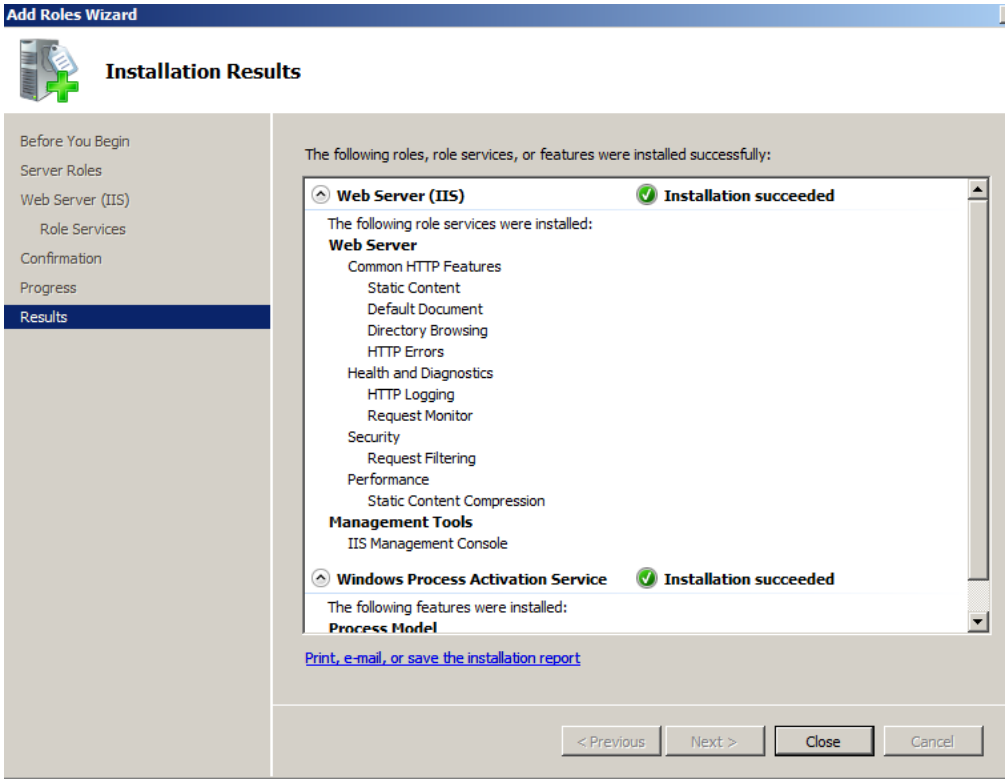
1. In Window's server open Start menu and go to Computer. Click on C:
2. While in C: create a new folder and name it profiles.
3. Right Click, on Profiles and go to Properties.
4. Under the Sharing tab click advanced sharing > share this folder > permissions > and click add.
5. Enter the name of the OU for the users you are authorizing and check the boxes read and change.
6. Click -> Ok -> Ok -> Close.
7. Under Start -> Administrative Tools -> Active Directory Users & Computers.
8. Click on grp5is375.edu3-> grp5OU3 ->User Properties -> Profile Tab
9. In the Profile Path text box type: \\grp5SRV \Profiles\grp5OU3user1 and so forth …
10. Repeat step 9 for each user in the OU

As a network administrator, can you view the content of each user's profile folder?

As an administrator, you have full access to view the files in this shared folder.

Task 15: Set up Web Server

• Add Web Server Role to your PDC using Server Manager. Attach a SS to show this is successful in your report.

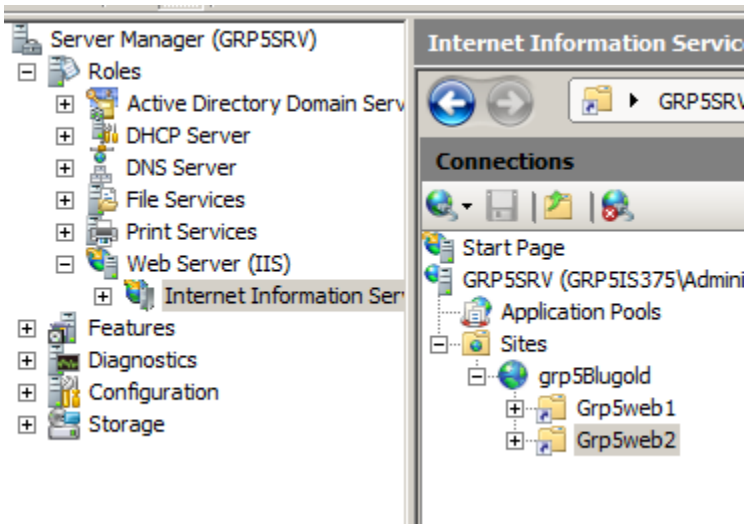


• For each of your web site including VD, you must have at least 1 sample html file as your default home page.

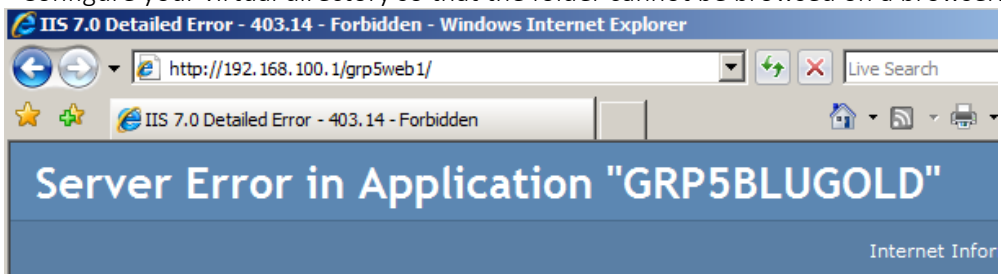
15.1 Default Web Site

• Name it grp5Blugold and create a host record for it on your DNS server.

• Then create two Virtual Directories (VD) with an alias name of Grp5web1 and Grp5web2 respectively.



• Configure your virtual directory so that the folder cannot be browsed on a browser.



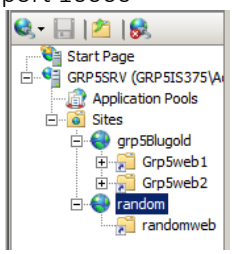
• Under what circumstances a virtual directory may be desirable?

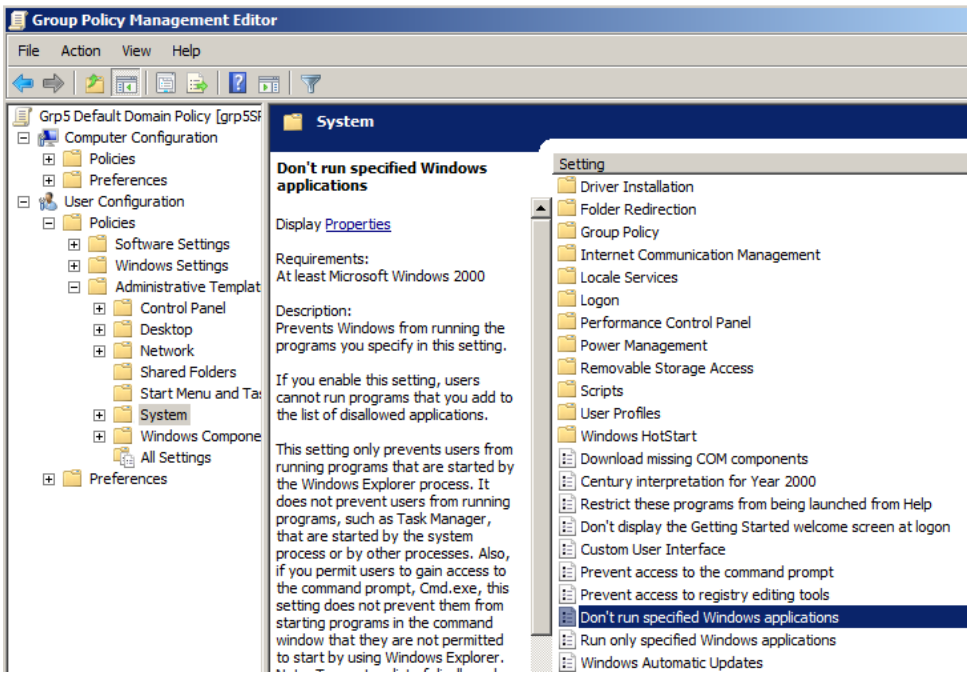
A virtual directory is a friendly name, or *alias*, either for a physical directory on your server hard drive that does not reside in the home directory, or for the home directory on another computer. Because an alias is usually shorter than the path of the physical directory, it is more convenient for users to type. The use of aliases is also secure because users do not know where your files are physically located on the server and therefore cannot use that information to modify your files. Aliases also make it easier for you to move directories in your site. Rather than changing the URL for the directory, you change the mapping between the alias and the physical location of the directory.

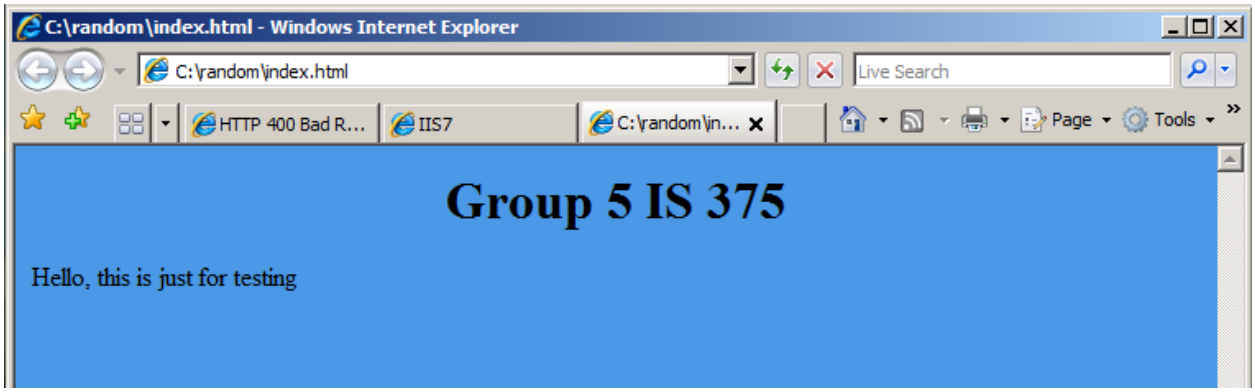
15.2 Create a second webs site on your server

• Create another web site on your server. Configure the TCP port to be 10000.

To create another website we disabled the Don't run specified programs in order to use notepad and create a html file to test what happens when you access random website if you don't include port 10000







• What happens when you access this web site if you don't include the port number in your URL?

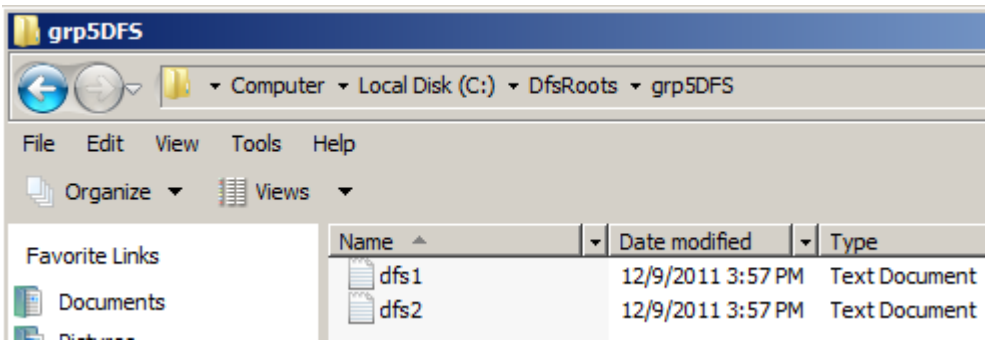
If you don't type the :10000 the website would resolve to port 80 as a http port default. So in order to open the random website we should type "https://192.168.100.1:10000/

Task 16: Set up DFS

• Refers to Activity 7-10 on Page 279 to add File Service and DFS role to your PDC. Using the following settings:

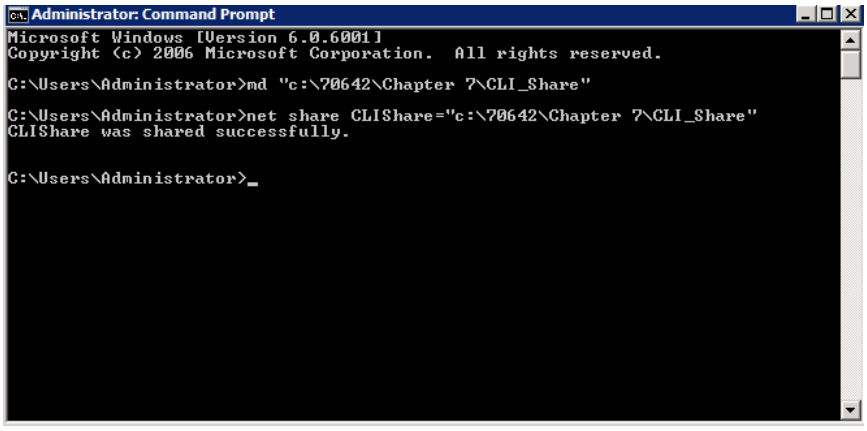
- DFS namespace: grp5DFS
- Type of Namespace: Domain-based
- Create 2 notepad files (dfs1.txt and dfs2.txt) within this grp5DFS folder on your C: drive.
- Where is grp5DFS located? Capture a SS.

Computer > Local Disk (C:) > DfsRoots > grp5DFS

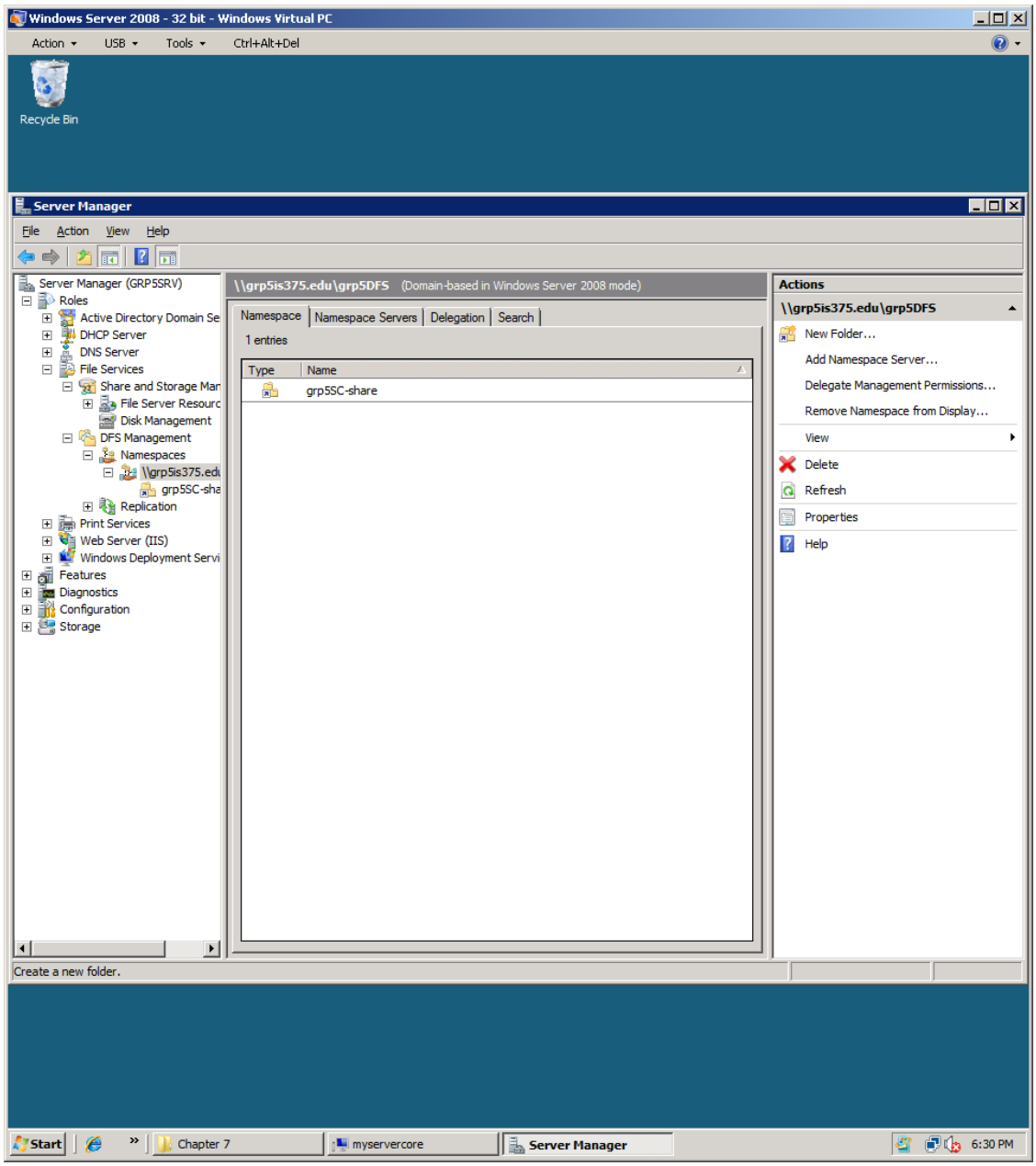


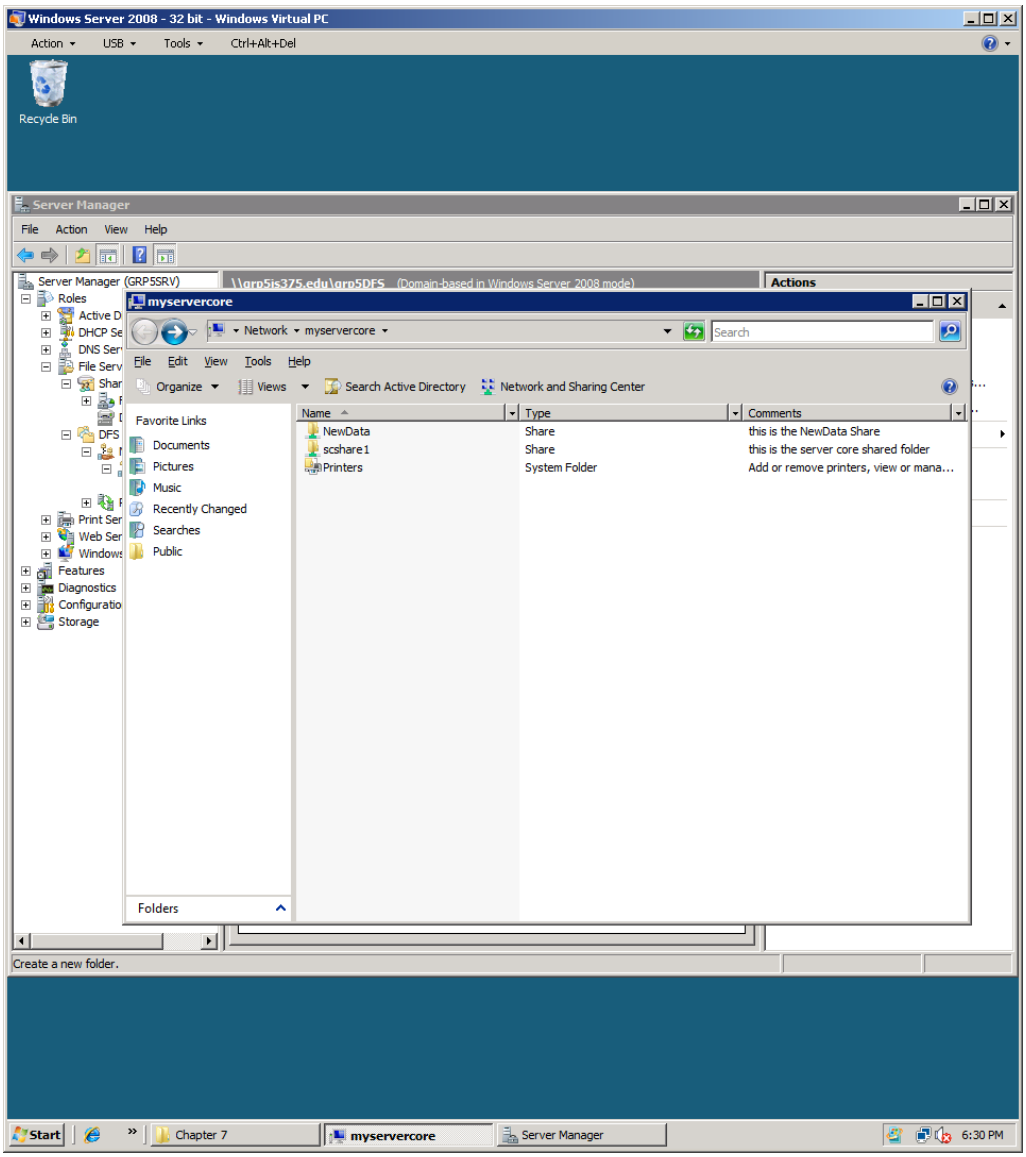
• In your report, explain why a domain-based DFS may be desirable to an enterprise network.
Benefits of domain-based DFS:

- Links together shared folders on different servers so they are organized to work as a single hard disk.
- Simplifies the transferring of data from one file server to another.
- High performance file servers can be deployed and used in new servers under existing namespaces.
- Can create multiple large namespaces without having to add more file servers to host.
- Has the ability to load share by mapping shared folders on different file servers.
- When a client wants to access a target, the information about the transaction is recorded on the client.
- If using Microsoft, you can enable the Offline Files feature for support.
- Administrators have the ability to do preventive maintenance, repair links, and upgrade servers.
- When using Window's 2000 DFS supports dynamic site discovery.
- Existing NTFS and share permissions on the links provide security for DFS namespaces.

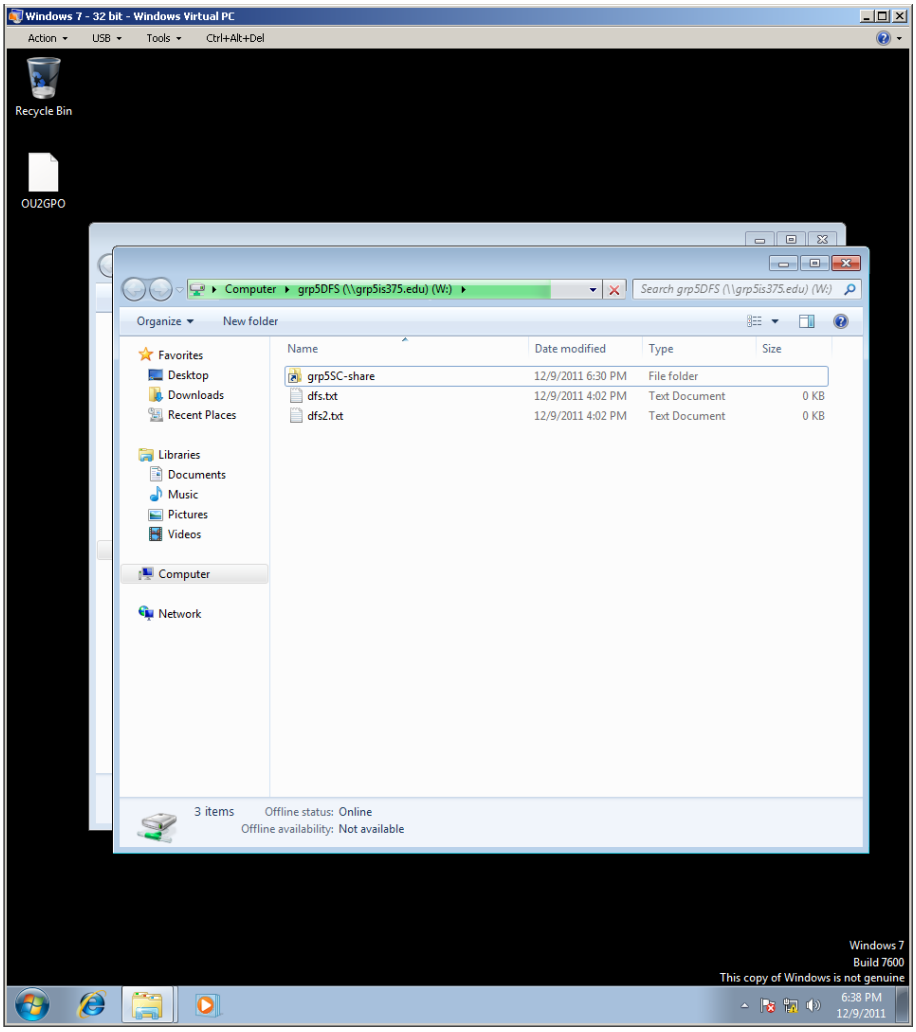


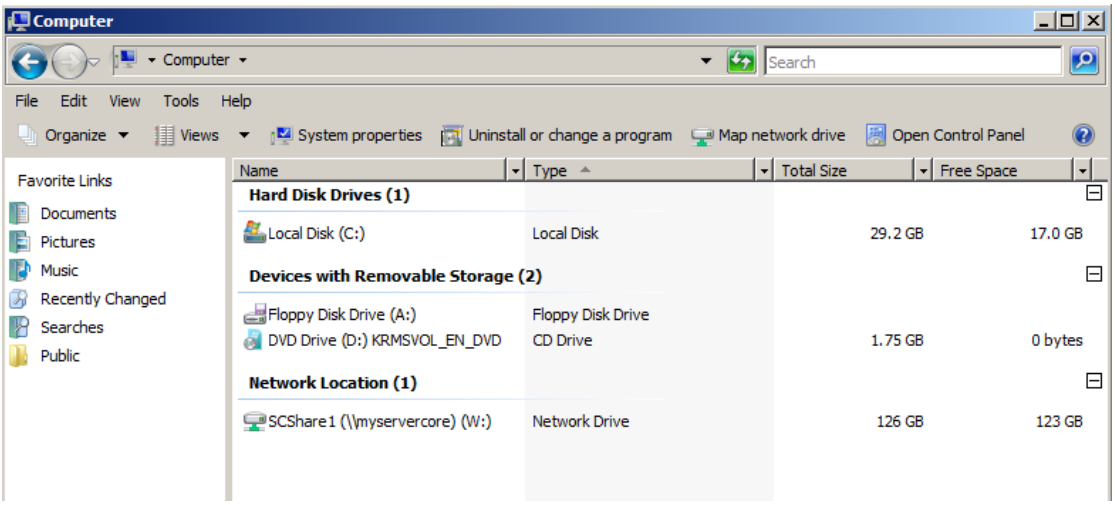
• On PDC, modify the namespace by creating a new folder named grp5SC-share, link it to your \\ServerCore \SCShare1 folder.


Windows Server 2008 - 32 bit - Windows Virtual PC
Action
USB
Tools
Ctrl+Alt+Del
Recycle Bin
Server Manager
File
Action
View
Help
Server Manager (GRP5SRV)
Roles
Active Directory Domain Se
DHCP Server
DNS Server
File Services
Share and Storage Mar
File Server Resourc
Disk Management
DFS Management
Namespaces
\\grp5is375.edu
grp5SC-sha
Replication
Print Services
Web Server (IIS)
Windows Deployment Servi
Features
Diagnostics
Configuration
Storage
\\grp5is375.edu\grp5DFS (Domain-based in Windows Server 2008 mode)
Namespace
Namespace Servers
Delegation
Search
1 entries
Type
Name
grp5SC-share
Actions
\\grp5is375.edu\grp5DFS
New Folder...
Add Namespace Server...
Delegate Management Permissions...
Remove Namespace from Display...
View
Delete
Refresh
Properties
Help
Create a new folder.
Start
Chapter 7
myservercore
Server Manager
6:30 PM



- On your W7, test the DFS by mapping a local drive W: to your grp5DFS share.
- Capture a SS to show the share contained in W:

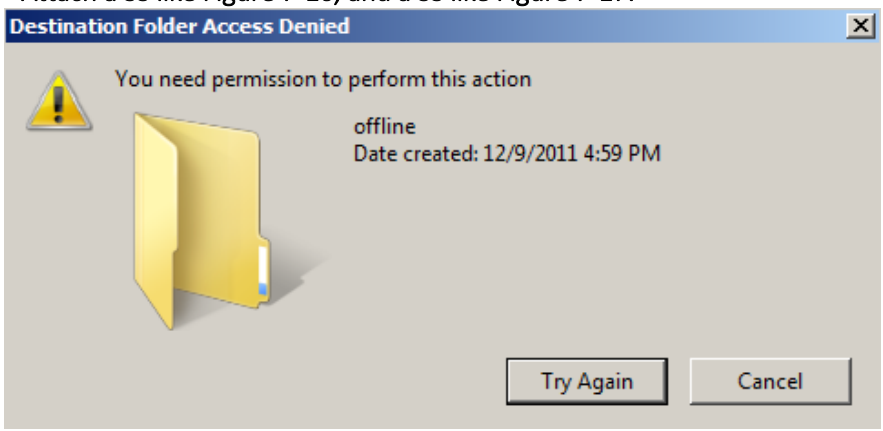

Windows 7 - 32 bit - Windows Virtual PC
Action
USB
Tools
Ctrl+Alt+Del
Recycle Bin
OU2GPO
Computer ▸ grp5DFS (\\grp5is375.edu) (W:) ▸
Search grp5DFS (\\grp5is375.edu) (W:)
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
grp5SC-share
12/9/2011 6:30 PM
File folder
dfs.txt
12/9/2011 4:02 PM
Text Document
0 KB
dfs2.txt
12/9/2011 4:02 PM
Text Document
0 KB
3 items
Offline status: Online
Offline availability: Not available
Windows 7
Build 7600
This copy of Windows is not genuine
6:38 PM
12/9/2011

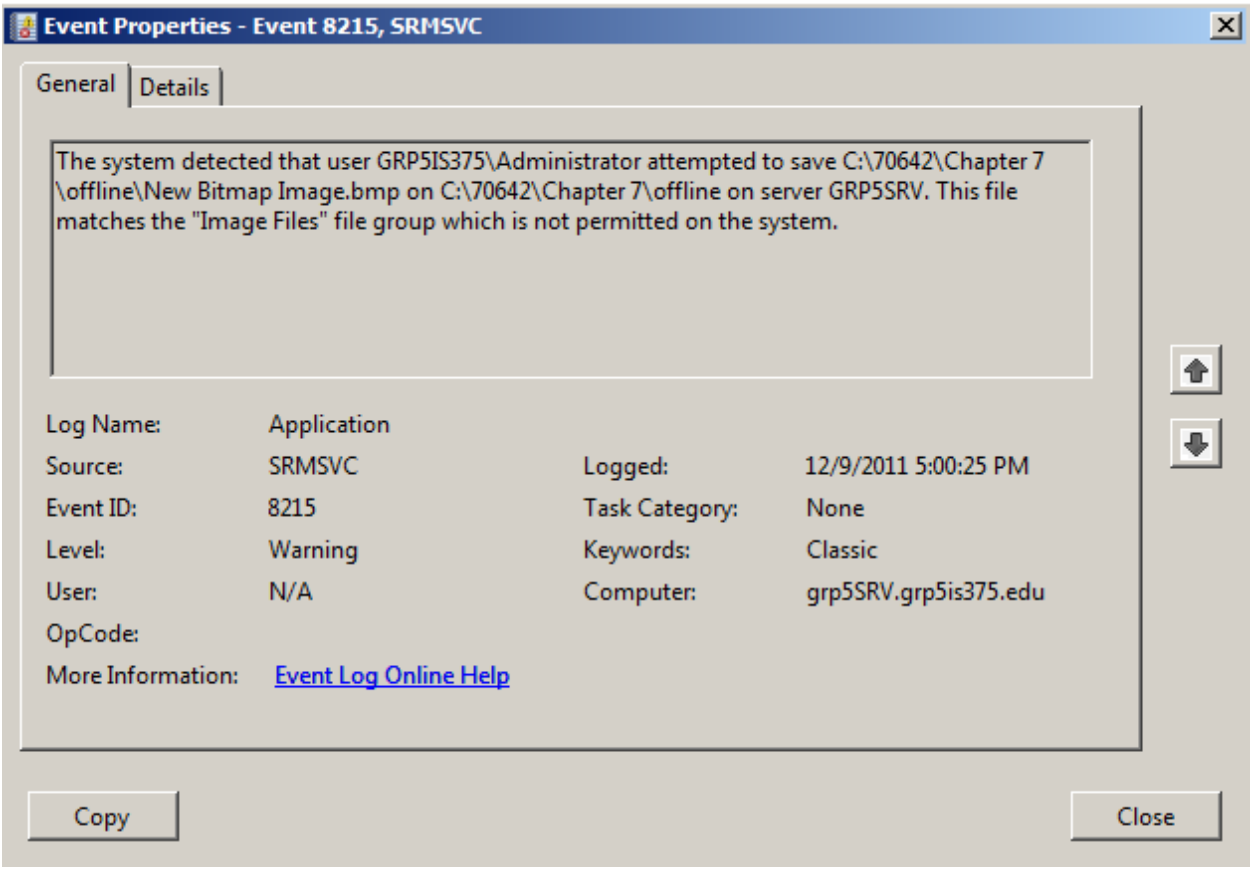

Computer
Computer
Search
File
Edit
View
Tools
Help
Organize
Views
System properties
Uninstall or change a program
Map network drive
Open Control Panel
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Name
Type
Total Size
Free Space
Hard Disk Drives (1)
Local Disk (C:)
Local Disk
29.2 GB
17.0 GB
Devices with Removable Storage (2)
Floppy Disk Drive (A:)
Floppy Disk Drive
DVD Drive (D:) KRMSVOL_EN_DVD
CD Drive
1.75 GB
0 bytes
Network Location (1)
SCShare1 (\\myservercore) (W:)
Network Drive
126 GB
123 GB

Task 17: On your PDC, block image files to be stored on your server, using FSRM.

• Refer to Activity 7-17 on page 290 for instructions.

• Attach a SS like Figure 7-16, and a SS like Figure 7-17.

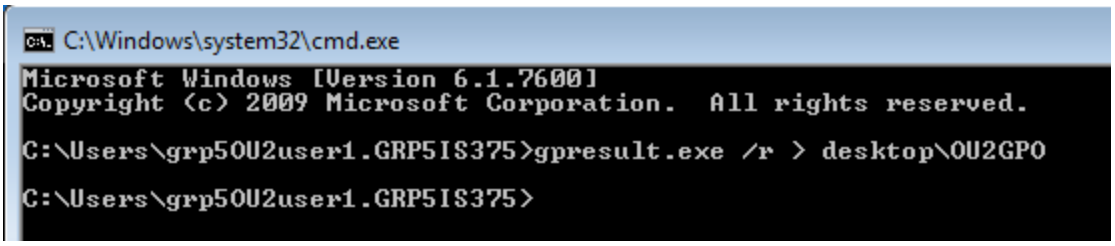




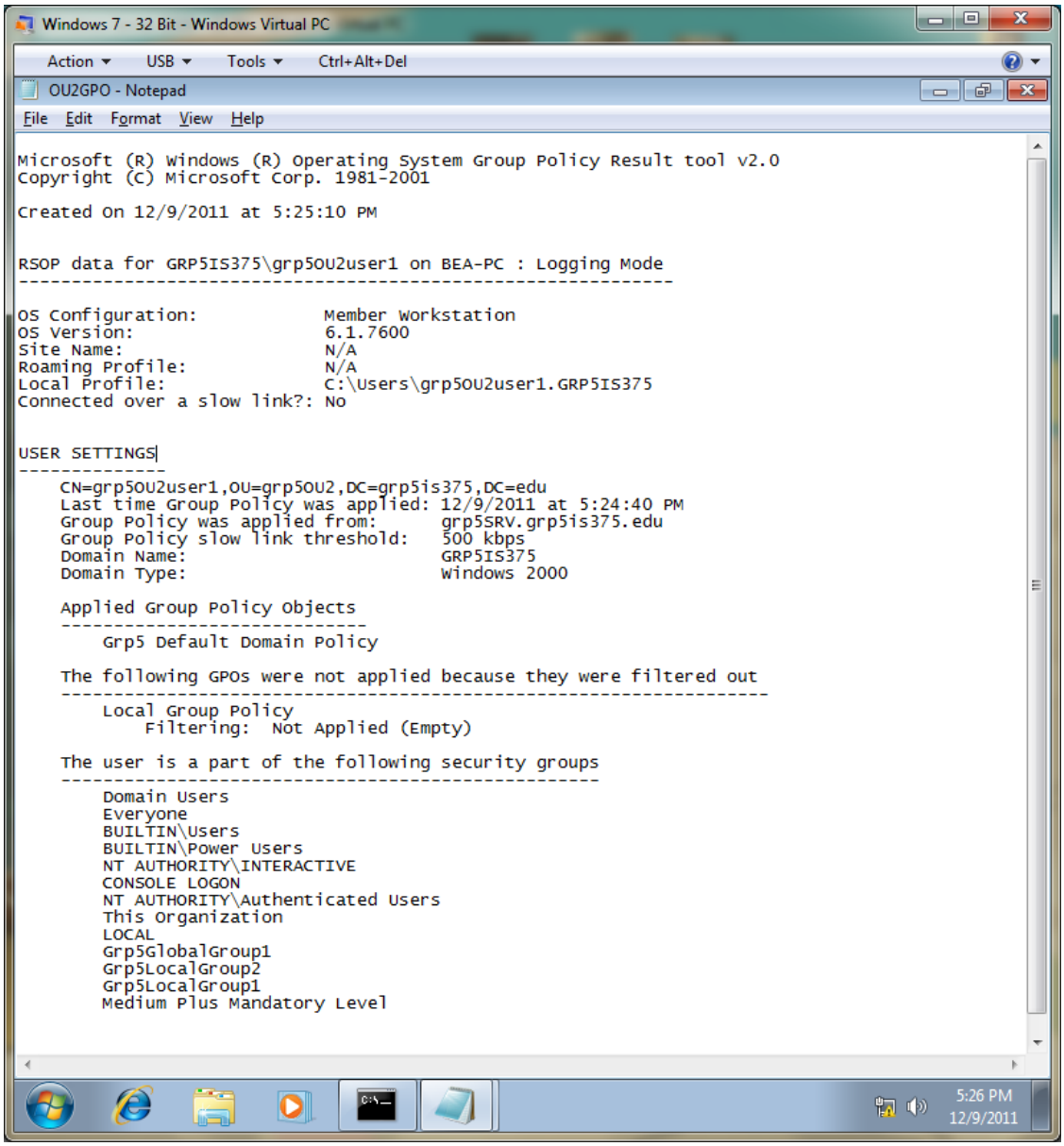
Task 18: On your Win 7, View effective GPOs Implementations Results.

Use the GPResult.exe /R utility.

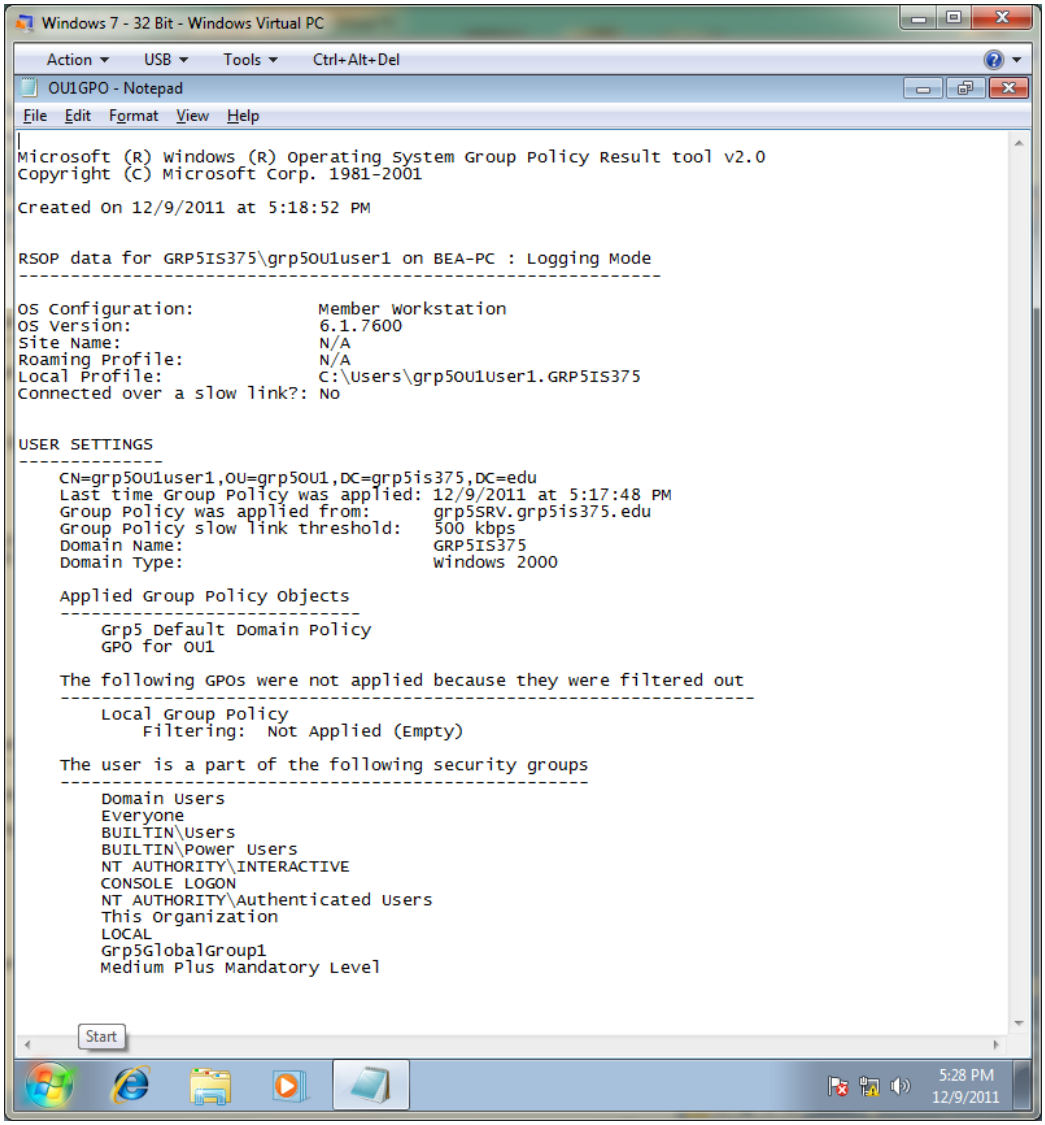
- View effective GPOs implemented on your XP client station, with a user account from OU2. Using the > switch to redirect the output to a notepad file named OU2GPO.
- View effective GPOs implemented on your XP client station, with a user account from OU1. Using the > switch to redirect the output to a notepad file named OU1GPO.
- Include the results in your project report as an appendix.


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\grp5OU2user1.GRP5IS375>gpresult.exe /r > desktop\OU2GPO
C:\Users\grp5OU2user1.GRP5IS375>

OU2GPO


Windows 7 - 32 Bit - Windows Virtual PC
Action
USB
Tools
Ctrl+Alt+Del
OU2GPO - Notepad
File Edit Format View Help
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001
Created On 12/9/2011 at 5:25:10 PM
RSOP data for GRP5IS375\grp5OU2user1 on BEA-PC : Logging Mode
OS Configuration: Member Workstation
OS Version: 6.1.7600
Site Name: N/A
Roaming Profile: N/A
Local Profile: C:\Users\grp5OU2user1.GRP5IS375
Connected over a slow link?: No
USER SETTINGS
CN=grp5OU2user1,OU=grp5OU2,DC=grp5is375,DC=edu
Last time Group Policy was applied: 12/9/2011 at 5:24:40 PM
Group Policy was applied from: grp5SRV.grp5is375.edu
Group Policy slow link threshold: 500 kbps
Domain Name: GRP5IS375
Domain Type: Windows 2000
Applied Group Policy Objects
Grp5 Default Domain Policy
The following GPOs were not applied because they were filtered out
Local Group Policy
Filtering: Not Applied (Empty)
The user is a part of the following security groups
Domain Users
Everyone
BUILTIN\Users
BUILTIN\Power Users
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Grp5GlobalGroup1
Grp5LocalGroup2
Grp5LocalGroup1
Medium Plus Mandatory Level
5:26 PM
12/9/2011

OU1GPO


Windows 7 - 32 Bit - Windows Virtual PC
Action
USB
Tools
Ctrl+Alt+Del
OU1GPO - Notepad
File Edit Format View Help
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001
Created On 12/9/2011 at 5:18:52 PM
RSOP data for GRP5IS375\grp5OU1user1 on BEA-PC : Logging Mode
OS Configuration: Member Workstation
OS Version: 6.1.7600
Site Name: N/A
Roaming Profile: N/A
Local Profile: C:\Users\grp5OU1User1.GRP5IS375
Connected over a slow link?: No
USER SETTINGS
CN=grp5OU1user1,OU=grp5OU1,DC=grp5is375,DC=edu
Last time Group Policy was applied: 12/9/2011 at 5:17:48 PM
Group Policy was applied from: grp5SRV.grp5is375.edu
Group Policy slow link threshold: 500 kbps
Domain Name: GRP5IS375
Domain Type: Windows 2000
Applied Group Policy Objects
Grp5 Default Domain Policy
GPO for OU1
The following GPOs were not applied because they were filtered out
Local Group Policy
Filtering: Not Applied (Empty)
The user is a part of the following security groups
Domain Users
Everyone
BUILTIN\Users
BUILTIN\Power Users
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Grp5GlobalGroup1
Medium Plus Mandatory Level
Start
5:28 PM
12/9/2011