# 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



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	No
		(dynamic)	

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	<ul> <li>Account lockout duration: an indefinite length</li> </ul>
<ul> <li>Maximum password age: 15 days</li> </ul>	of time
<ul> <li>Minimum password age: 5 days.</li> </ul>	<ul> <li>Account lockout threshold: 3 invalid logon</li> </ul>
<ul> <li>Minimum password length: 7</li> </ul>	attempts
<ul> <li>Passwords must meet complexity</li> </ul>	• Reset account lockout count after: 60 minute
requirements: enabled	

### 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

Administrator: C:\Windows\system32\cmd.exe	
C:\Users\Administrator>ipconfig /all	
Windows IP Configuration	
Host Name : grp5SRU Primary Dns Suffix : grp5is375.edu Node Type : Hybrid IP Routing Enabled : No WINS Proxy Enabled : No DNS Suffix Search List : is375.edu	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix .: Description Intel 21140-Based PCI Fast Ethernet er (Emulated)	Adapt
Physical Address 00-03-FF-00-EE-1C DHCP Enabled	ed)
DNS Servers	
Tunnel adapter Local Area Connection* 8:	
Media State Media disconnected Connection-specific DNS Suffix . : Description : isatap.{21E7FD19-1675-4EB9-BE18-0550 3A4} Physical Address	40353
Hutoconfiguration chapted Yes	
Media State	
C:\Users\Administrator>	

🖬 Administrator: C:\Windows\system32\cmd.exe
C:\Users\CoreAdmin>ipconfig /all Windows IP Configuration Host Name : myservercore Primary Dns Suffix : grp5is375.edu Node Type Hybrid IP Routing Enabled : No WINS Proxy Enabled : No DNS Suffix Search List : grp5is375.edu
Connection-specific DNS Suffix : Description
Tunnel adapter Local Area Connection*: Media State Media disconnected Connection-specific DNS Suffix . : Description : isatap. <c1b38054-124e-41f5-863c-be22336e9 6FF) Physical Address : 00-00-00-00-00-00-E0 DHCP Enabled No Autoconfiguration Enabled : Yes C:\Users\CoreAdmin&gt;_</c1b38054-124e-41f5-863c-be22336e9 

### 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

Windows Server Core - Windows Virtual PC
Action ▼ Tools ▼ Ctrl+Alt+Del
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator>netsh interface ipv4 add dnsserver "local area connection" " 192.168.100.1
C:\Users\administrator>ipconfig /all
Vindows IP Configuration
Host Name : MyServerCore Primary Dns Suffix : Node Type : Hybrid IP Routing Enabled : No WINS Proxy Enabled : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix .: Description
funnel adapter Local Area Connection*:
Media State Media disconnected Connection-specific DNS Suffix . : Description : isatap.{FD402140-01C4-42CE-AF8D-D40085A2FC DB0 Physical Address : 00-00-00-00-00-00-E0
DHCP Enabled No Autoconfiguration Enabled : Yes
Tunnel adapter Local Area Connection* 3:
Media State : Media disconnected Connection-specific DNS Suffix . : Description : Teredo Tunneling Pseudo-Interface Physical Address : 802-00-54-55-4E-01 DHCP Enabled : No Outcoonfiguration Enabled : No

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

👞 Administrator: C	:\Windows\system32\cmd.exe	×
Windows Server curity setting .0." This sett m using weaker hannel session	2008 domain controllers have a new more secure default for the se named "Allow cryptography algorithms compatible with Windows NT 4 ing prevents Microsoft Windows and non-Microsoft SMB "clients" fro NT 4.0 style cryptography algorithms when establishing security c s against Windows Server 2008 domain controllers. As a result of t	
iced by Window	📗 rodcpromo - Notepad	
Platforms impa ft SMB "client stronger crypt Windows earli ain join opera Deployment Ser For more infor ://go.microsof This computer any of its ne apter, both IH d IPv6 Propert an IPv6 Stati ess(es) for re atic IP addres ler and any de ess will stop You must resta C:\Users\admir C:\Users\admir	File Edit Format View Help [DCINSTALL] InstallDNS=Yes ConfirmGc=No CriticalReplicationOnly=No DisableCancelForDnsInstall=No Password= RebootOnCompletion=No ReplicaDomainDNSName=grp5is375.edu ReplicaorNewDomain=ReadOnlyReplica SafeModeAdminPassword= SiteName=Default=First=Site=Name UserDomain=grp5is375.edu Username=Administrator	

📕 Server Manager						
File Action View Help						
🗢 🔿 🙍 🖬 🖬 🖬 🔹	3					
Server Manager (GRP5SRV)	Domain Controllers	2 objects [Filter Ad	:tivated]		Actions	
🖃 💕 Roles	Name	Туре	DC Type	Site	Domain Controllers	•
Active Directory Domain Se     Active Directory Users ;     Active Directory Users ;     Active Directory Users ;     Builtin     ①    Builtin     ①    Computers     ②    Domain Control     ①    ForeionSecurity	N GRP5SRV	Computer Computer	GC Read-only, DC	Default Default	More Actions	۶

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 There are currently no logon servers available to service the logon request OK

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.

🕌 project		_ 🗆 🗵
G 🕞 - 🚺 - Computer	r • Local Disk (C:) • project • • • 😧 Search	<u> </u>
File Edit View Tools H	reip ▼ ■ Open 👷 Share	0
Favorite Links	Induce     Image     Image       pp55hare1     12/8/2011 12:2:     File Folder       pp55hare2     12/8/2011 12:2:     File Folder       pp55hare3     12/8/2011 12:2:     File Folder       pp55hare4     Sharng     Securty       Object name:     C'upoject'upp5hare3     Group or user names:       % CREATOR OWNER     % SYSTEM       % Administrators (GRPSIS375/Administrators)     %       % Users (GRPSIS375/Users)     To change permissions, click Edt.       To change permissions, click Edt.     Edt       Permissions for Users     Allow       Modify     K       Read     V       Write     V       Special permissions     V	
Folders ^	click Advanced.	
	Learn about access control and permissions           OK         Cancel         Apply	

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.

🐂 Server Hanager		Server Manager					
File Action View Help		File Action View Help					
(= =) 2 10 4 🛛 🗙 🗊 2 🕞 🗳 🖬 🗤		🗢 🔿 🙍 📷 🔏 🗖 🗙 🖫	2 🕒 🖬 🖬				
Server Manager (CRPSSRV) OUTorGroups 4 objects (Filter Activated)	Actions	Server Manager (GRPSSRV)	OUTorGroups 4 obj	ects (Filter Activates	1	Actions	
P Roles     Name     Type     Description     C	OUforGroups	Roles	Name	Type	Description	OUforGroups	
Active Directory Domain Se     Active Directory Users     Active Directory Users	More Actions	Active Directory Domain Se Active Directory Users.	GrpSLocalGroup1	Security Group	,	More Actions	•
grg 5s375.edu     Score and a state a	Grp5GlobalGroup1	grp5is375.edu	ScroSGobalGroup 2	Security Group		Grp5GlobalGroup2	
R Computers & GrpSLocalGroup2 Security Group	Nore Actions	E Computers	& Grp5GlobalGroup2	Security Group		More Actions	•
8 🚊 Domain Control		(8) 🗾 Domain Control					
I ForeignSecurity		ForeignSecurity				L	a local
B grp5s375.edu	<u>1×</u>	R grpss375.e00		rp5GlobaKroup2	Properties		<u>1</u> ×1
8 grp50U2 General Members Member Of Managed By		grp5OU2		General Members	Member Of Managed By		
If grp50U3 Members		grpSQU3		Members:			
OUTOGROUPS     Nome Active Directory Domain Service	ices Folder	Users		Name	Active Directory Domain 5	Services Folder	7
Active Directory Sites a     Sop 50011user1 gp5s375.edu/gp5001/gp5	50U11	Active Directory Sites a		💄 grp50U11us	er4 gp5is375.edu/gp50U1/	gp50U11	
E PDP Server Sp5s375.edu/gp50U1/gp5	50U11	DHCP Server		\$ 9p50U11us	er5_gp5is375.edu/gp50U1/	gp50U11	
E Spoultures server Spoultures applications and applications and applications applications and applications	50011	(i) Services		s gp5001use	r4 gpbs3/5.edu/gpb001 r5 gp5s375.edu/gpb001		
gp501/0eer/gp501/3eeu/gp501/     gp501/0eer/gp501/3eeu/gp501/1     gp501/0eer/gp501/3eeu/gp501/1		(i) (iii) Print Services		50U2use	r4 gp5s375.edu/gp50U2		
		E of Features		S gp50U2use	r5 gp5s375.edu/gp50U2		
E m Dagnostics gp50U2.ser1 gp5s375.edu/gp50U2		Configuration		👗 grp50U3use	r4 gp5is375.edu/gp50U3		
B gp50U2use2 gp5s375.edu/gp50U2		🗉 🧱 Storage					
5 gp50U2user3 gp5s375 edu/gp50U2							
gp5603aar gp56375edu/gp5003							
🖁 gp50U3user3 gp5is375.edu/gp50U3							
Add Denses				Add	Remove		
Add Herroyc							
OK Ca	ancel Apply				ок	Cancel Apply	

### 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

Shared Poloers Start Menu and System Windows Comp Comp All Settings	Windows from searching for updates.       If you disable or do not configure it,         If you disable or do not configure it,       Restrict these programs from         Windows searches for updates and automatically downloads them.       Image: Restrict these programs from	nd prompt being launched from Help pplications
🕀 📔 Preferences 📃 🔽	Note: Windows Automatic Updates Properties	? ×
	Exten Setting Explain Comment Comment	

# 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 <u>local Administrators</u> group. And, make the Grp5gloablgroup1 a member of the local <u>Power Users</u> group.

😣 lusrmgr - [Local Users and Grou	ips (Local)\Groups]							
File Action View Help		🥼 lusrmgr - [Local Users and Group	s (Local)\Groups]					
🗢 🄿 🖄 📅 🗶 🕞 🔒		File Action View Help						
Local Users and Groups (Local)	Name Description							
Groups	Administrators Administrators have complete an	💭 Local Users and Groups (Local)	Name Description					
	Backup Operators Backup Operators can override se Cryptographic Operat Members are authorized to perfor	Users Groups	Administrators	Administrators have complete an	G	roups		
	Distributed COM Users Members are allowed to launch, a		Backup Operators	Backup Operators can override se.		Mon		
Adm	ninistrators Properties		🕭 Di 🛛 Power Users Proj	perties	? ×	wer Us		
Ge	neral		Ev General			More		
A A A A A A A A A A A A A A A A A A A	Administrators		A IS A Ne A Pow	er Users				
	escription: Administrators have complete and unrestricted access to the computer/domain		Pe Description:     Pe     Pe     Re     Members:	Power Users are included for backwards compatibility and possess limited administrative powers				
	Administrator     Boa     GRPI3375/DLocalGrp1     GRPI3375/DLocalGrp1     GRPI3375/DLocalGrp1     GRPI35375/Dumain Admine     GRPI35375/DisbalGroup2     GRPI35375/Glp5GlobalGroup2     GRPI35375/UhrvGrp1     Sp-5-21-1849476305-4015751718-3538514166-1113		A Re Us Us Us	75\Grp5GiobalGroup1				
	Add Changes to a user's group membership are not effective until the next time the user logs on.		Add	Changes to a user's gro are not effective until th user logs on.	up membership ie next time the			
	OK Cancel Apply Help			OK Cancel Apply	Help			
					1	1		

### 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.

Name 🔺		- Date modi	fied	<ul> <li>Type</li> </ul>		▼ Size	-	Tags	-
📗 grp5share 1		10/0/0011	10.02	Eilo Colda	~			_1	
🔰 grp5share2	ירא ופ 👆	marcarrup	CILICS					<u>×</u> ا	
🍌 grp5share3	Genera	Sharing	Security	Previous V	ersions	Customi	ze		
	C	Permission	s for ar	n5chare1				¥1	1
	_	CHINSSION	s ior gi	positierer					
	r S	ecurity							
		Object name:	C:\pr	roject\grp5sh	iare1				
		Group or use	r names:						
	L	& CREAT	OR OW	VER					
	Т	& SYSTEI	M						
	F	🍇 Administ	rators (G	RP5IS375\A	dministr	ators)			
	ċ	Scrp5Loo	alGroup	1 (GRP5IS3)	75\Grp5	LocalGro	up 1)		
	Г	Sers (G	RP5IS3	75\Users)					
					Ad	d	Remov	re	
		Permissions f	or Grp5L	.ocalGroup1		Allow	Deny		
		Full contro						•	
	F	Modify					H		
	c	Read & ev	ecite				H		
		Liet folder	contente				H		
	L	Dand	Contentes				H		
	_	nodu .				<u>ت</u>			
		Leam about a	access c	control and pe	emission	<u>15</u>			
			Г	OK		Canaal	1 0-	-	
			L	UK		Cancel	A	ру	
									3

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

SIUIIS. GIV	only read share permission.	
• Don't a	low any other users to access this shar	e.
🛛 🐌 grp5share	12/8/2011 12:23 File Folder	
grp5shar grp5shar	grp5share2 Properties	
	eneral Sharing Security Previous Versions Customize	
	Permissions for grp5share2	
	G Security	
	Object name: C:\project\grp5share2	
	Group or user names:	
	A SECREATOR OWNER	
	- Administrators (GRP5IS375\Administrators)	
	C & Grp5LocalGroup2 (GRP5IS375\Grp5LocalGroup2)	
	Users (GRP5IS375\Users)	
	Add Remove	
	Permissions for Grp5LocalGroup2 Allow Deny	
	Modify	
	F Read & execute	
	List folder contents	

### • 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.

Add Roles Wizard		
Installation Resu	lts	
Before You Begin Server Roles Web Server (IIS) Role Services Confirmation Progress Results	The following roles, role services, or features were installed successfully:	
	< Previous Next > Close	Cancel

• 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.

C ≥   + 2 http://192.168.100.1/grp5web1/	🔽 🐓 🗙 Live Search
😭 🏟 🍘 IIS 7.0 Detailed Error - 403. 14 - Forbidden	🚹 • 🗟 - 🖶 ·
Server Error in Application	"GRP5BLUGOLD"
	Internet Info

### • 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





	1-		 A
	Group 5	IS 375	
Hello, this is just for testing			

- 🗆 ×

<del>-</del> و

 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

🔒 grp5DFS				
Computer ★ Local Disk (C:) ★ DfsRoots ★ grp5DFS				
File Edit View Tools Help				
🕒 Organize 🔻 🏢 Views 👻				
Favorite Links	Name 🔺 🚽 Date modified 💌 Type			
	dfs1 12/9/2011 3:57 PM Text Document			
Documents	dfs2 12/9/2011 3:57 PM Text Document			
Pint man				

• 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.





- 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:





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.	
Destinati	ion Folder Access Denied	×
	You need permission to perform this action offline Date created: 12/9/2011 4:59 PM	
	Try Again Cancel	

Imatches the Image Files file group which is not permitted on the system.         Log Name:       Application         Source:       SRMSVC       Logged:       12/9/2011 5:00:25 PM         Event ID:       8215       Task Category:       None         Level:       Warning       Keywords:       Classic         User:       N/A       Computer:       grp5SRV.grp5is375.edu         OpCode:       More Information:       Event Log Online Help	General Details	ed that user GRP5IS375\Adm ap Image.bmp on C:\70642\(	inistrator attempted t Chapter 7\offline on s	o save C:\70642\Chapter 7 erver GRP5SRV. This file	-
Source:       SRMSVC       Logged:       12/9/2011 5:00:25 PM         Event ID:       8215       Task Category:       None         Level:       Warning       Keywords:       Classic         User:       N/A       Computer:       grp5SRV.grp5is375.edu         OpCode:       More Information:       Event Log Online Help	Log Name:	Application	ot permitted on the s	ystem.	<u>+</u>
Event ID:     8215     Task Category:     None       Level:     Warning     Keywords:     Classic       User:     N/A     Computer:     grp5SRV.grp5is375.edu       OpCode:     Keywords:     Event Log Online Help	Source:	SRMSVC	Logged:	12/9/2011 5:00:25 PM	
Level:     Warning     Keywords:     Classic       User:     N/A     Computer:     grp5SRV.grp5is375.edu       OpCode:	Event ID:	8215	Task Category:	None	
User: N/A Computer: grp5SRV.grp5is375.edu OpCode: More Information: Event Log Online Help	Level:	Warning	Keywords:	Classic	
OpCode: More Information: <u>Event Log Online Help</u>	User:	N/A	Computer:	grp5SRV.grp5is375.edu	
More Information: <u>Event Log Online Help</u>	OpCode:				
	More Information:	Event Log Online Help			
	1				

### 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.



### OU2GPO

💐 Windows 7 - 32 Bit - Windows Virtual PC	
Action ▼ USB ▼ Tools ▼ Ctrl+Alt+Del	• 🕥
OU2GPO - Notepad	
<u>F</u> ile <u>E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp	
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\grp50U2user1.GRP5IS375 Connected over a slow link?: No	
USER SETTINGS CN=grp50U2user1,0U=grp50U2,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 	11
<	-
🚱 🖉 🚞 🖸 🔤 🔍	● 5:26 PM 12/9/2011

### OU1GPO

