**Secure Microsoft Windows**

**Practical 3**

**Configuring and Managing Resource Access**

|  |
| --- |
| **Objectives:**  After completing this lab, you should be able to:   1. Joining a Windows 2012R2 server to a Domain 2. Configuring Folder Permissions 3. Enable Network Discovery and Shared Folder feature using SCW 4. Configuring Shared Folder Permissions 5. Understand the operations of security groups. 6. Setting up Encrypting Files and the basic usages of the Cipher command 7. Audit Options for File Folders 8. Try simple Powershell commandlets 9. View User Profiles and set a Roaming Profile |
|  |

Lab Prerequisites:

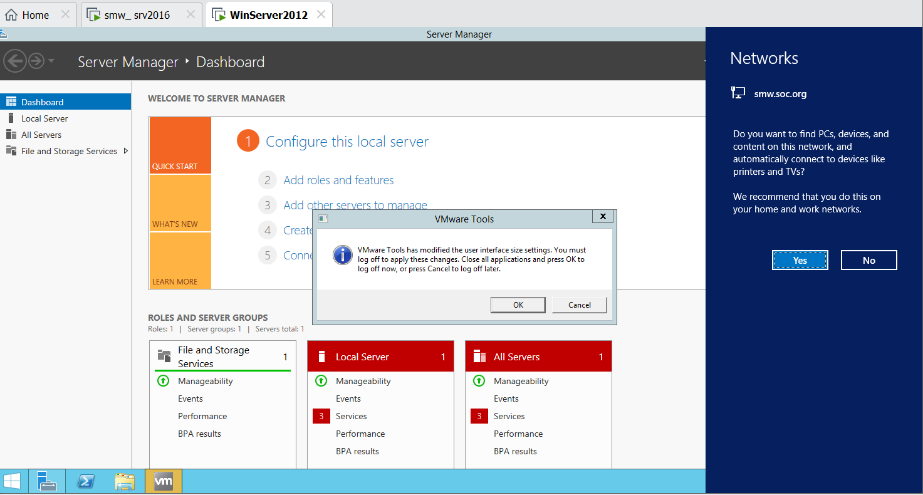
Completion of the Lab exercises on Practical 2.

Domain User account : Mgr1 has been created successfully.

The Base image of the Windows 2012R2

**Lab exercise 3-0: Adding a new member server (Windows 2012R2) to your domain**

1. Start your Domain Controller
   * You need to start your Domain Controller as it provide the essential DNS and DHCP services to the VM within your NAT segment.
   * You do not need to start your Windows 10 client. (To reduce the resources)
   * Caveat : If you have forgotten to disable the vmware local dhcp services, you may encounter many mysterious issues due to the inconsistent of DNS and DHCP services.
2. After the Domain Controller has been started (with the Server Manager loaded ). You may start your Windows 2012R2 VM.
   * The default login / password of the Windows 2012R2
     + ladmin / 1qwer$#@!



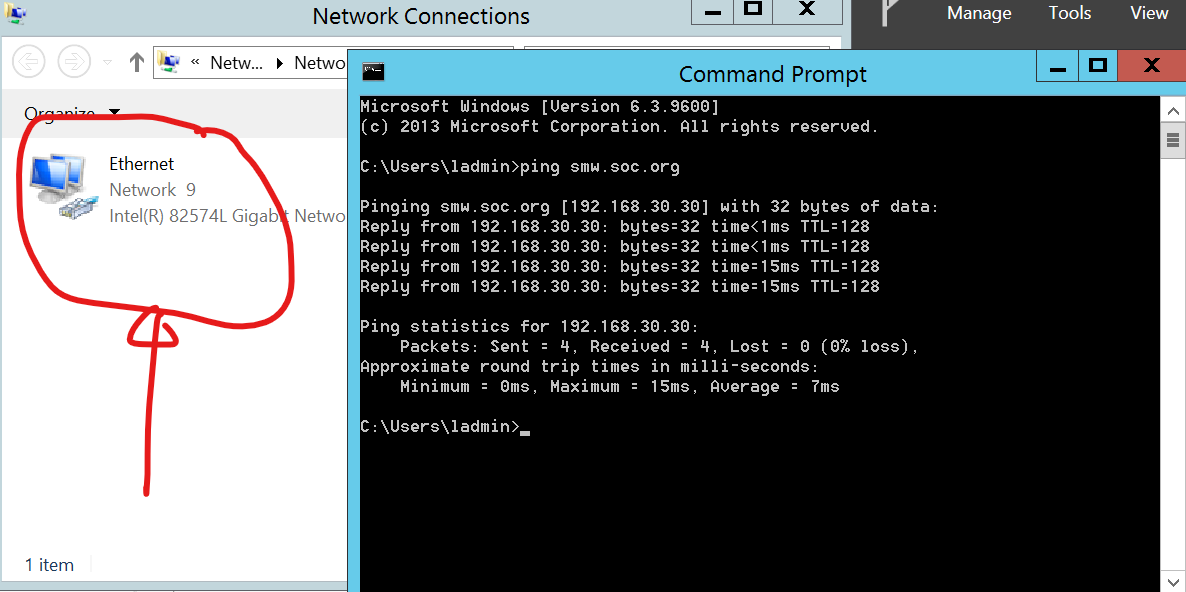
At the first run of your new VM, your may see the Network Connection and the vmware tools popup. It is normal. After cleared the vmware tools popup, your VM may force to sign out to let the new display resolution settings kicks in. Login to ladmin again.

Proceed to carry out the necessary steps to configure an additional Windows 2012R2 server to join into your domain.

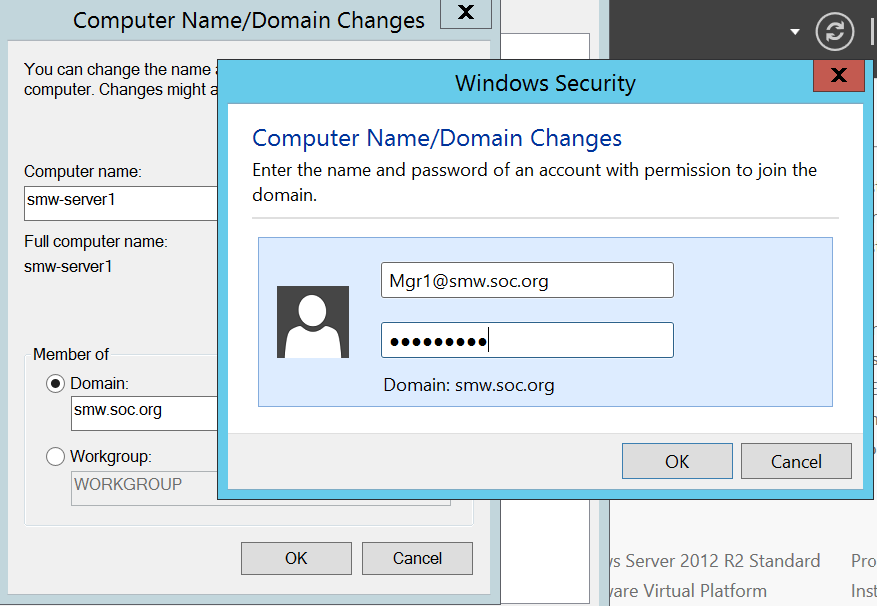
In initially, your server 2012R2 is based on Dynamic IP. Decide a set of static IP values to this server.

* + Ensure you are assigning a reasonable static IP address to this server.
    - List down the following of your new server:
      1. Computer Name \_\_\_\_Leo\_memsrv\_1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
      2. Static IP address \_\_\_\_192.168.126.55\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
      3. Network Mask \_\_\_\_\_\_255.255.255.0\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
      4. Gateway \_\_\_\_\_\_\_\_\_\_\_192.168.126.2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
      5. Preferred DNS \_\_\_\_\_\_192.168.126.90\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  + Verify your new server can
    - access to the Internet
    - ping your FQDN (e.g. smw.soc.org)

before joining the domain.

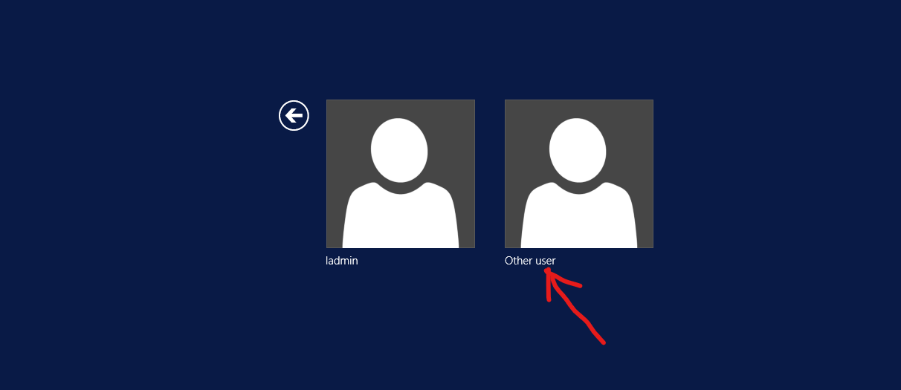


* + Proceed to change your server name and join to the domain. When being prompt for the Authentication before joining to the domain, try to use the Mgr1 credential. (By default, any authenticated domain account can bring in new domain member machine !)



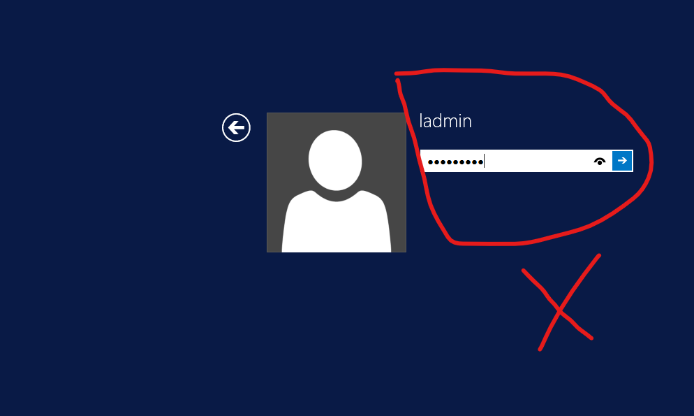
* + Using the BPA to check this new member server. (optinal / can defer)
  + Verify your new server can access to the Internet after joining the domain.

1. Verify your setup by logging on the new member server with the following Domain user accounts (you have created in the previous practical exercises):
   * Mgr1, Staff1, and User1



Click on the Other user link, then you can type in the user id for your login.

* + In fact, you should avoid to use ladmin account to login to this server. As ladmin remains as the local administrator of the server. It is not sufficient if you want to carry out domain level administrative task. (ladmin becomes a backup / fallback account)



Reflection prompt: Based on your observations, comment on the difference between the two BPA scanning results of the Domain Controller and this new member server.

The BPA scan from the domain controller shows all the issues in the domain while the BPA scan in the new member server only shows issues for the new member server.

**Lab exercise 3-1**

Login as different Domain user accounts at the Windows 2012R2 member server to carry out the following 3-1 (a-d) exercises.

**Lab exercise 3-1a: Encrypting Files**

**3-1a.1**

Login in as User1 to create and encrypt files in a folder.

Refer to Activity 5-2 of the textbook for the step by step instructions of this exercise.

At step 1: Navigate to C:\Users\User1\Documents to start this exercise.

**3-1a.2**

**Try to use cipher command at to:**

**Display EFS status at folder and file level**

**Encrypt files**

**Decrypt files**

Reflection Prompt: Can you verify how to apply –W option with the Cipher command, and explain what is the use of it ?

**Lab exercise 3-1b: Configuring Folder Permissions**

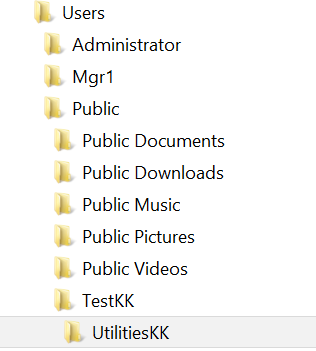
Login in as User1 to create a folder and grant modify permission of this folder to other user via security group.

Refer to Activity 5-3 of the textbook for the step by step instructions of this exercise.

At step 1: Navigate to C:\Users\Public to start this exercise.

After the completion of step 1, you should have (using User1 account) created the C:\Users\Public\TestXX\UtilitiesXX folder. (XX is your initials)

!read the above path carefully!



At step 5: Go to find the ‘DomainMgrs’ group instead of the ‘Server Operators’ group.

At step 6. What permissions do the DomainMgrs have by default ?

Graphical user interface

Description automatically generated

At step 7. Grant the Modify permission of UtilitiesXX to DomainMgrs.

**Lab exercise 3-1c: Inherited Permissions**

Before proceed to work on this exercise, try to login to the Windows 2012R2 server with Mgr1 and Staff1 accounts. Find out if these two accounts can both navigate to the C:\Users\Public\TestXX\UtilititiesXX folder. Record down your findings and login as User1 again to proceed.

Both are able to access

Refer to Activity 5-4 of the textbook for the step by step instructions of this exercise.

At Step 6. Confirm (instead of cancel) the Remove all inherited permission from this object (i.e. UtilitiesXX).

Now login as Mgr1 and Staff1 again to try to navigate to the C:\Users\Public\TestXX\UtilititiesXX folder. Compare your results with the previous experiment. Do you see any difference? Can you explain?

Mgr1 is able to access while Staff1 is unable to access. User 1 also unable to access

**Lab exercise 3-1d: Configuring Advanced Permissions**

Refer to Activity 5-5 of the textbook for the step-by-step instructions of this exercise.

Try to answer the following question:

* At Step 16, what does “Apply these permissions to objects and/or containers within this container only” mean?

Permissions won’t cascade for more than 1 level

**Lab exercise 3-1e: Verifying the effect of Deny Permissions.**

1. Login in as a Domain Admin to your DC.
2. Ensure you have the following 2 global groups in your domain: GlobalMgrs, GlobalStaff

(Create them accordingly).

1. Create a new Domain user account : newManager.
2. Add newManager to both of the GlobalMgrs and GlobalStaff global groups.
3. Ensure you have the following 2 domain local groups in your domain: DLMgrs, DLStaff.

(Create them accordingly)

1. Add GlobalMgrs group to DLMgrs.
2. Add GlobalStaff group to DLStaff.
3. Switch to the member server 2012R2, Login as Domain Admin.
4. Create a file, testDeny.txt, at the C:\Users\Public\TestXX\ folder.
5. Assign the full control permission of the testDeny.txt to DLMgrs.
6. Assign the read control permission of the testDeny.txt to DLStaff.
7. Switch the login to newManager at the member server2012R2.
8. Test if newManager can update the testDeny.txt file.
9. As newManger, try to add Deny Read permission to DLStaff group for the file, testDeny.txt

(If fail to do so, you may need to switch back to Domain Admin to add the permission)

1. Test if newManger can update the testDeny.txt file after step 14.

Access is denied

Graphical user interface, application

Description automatically generated

Note: At times, it is always easier to view the Account - Groups - Permission relationship with a diagram.

For example, we can summarize the 3-1e group assignment configuration in the following diagram.

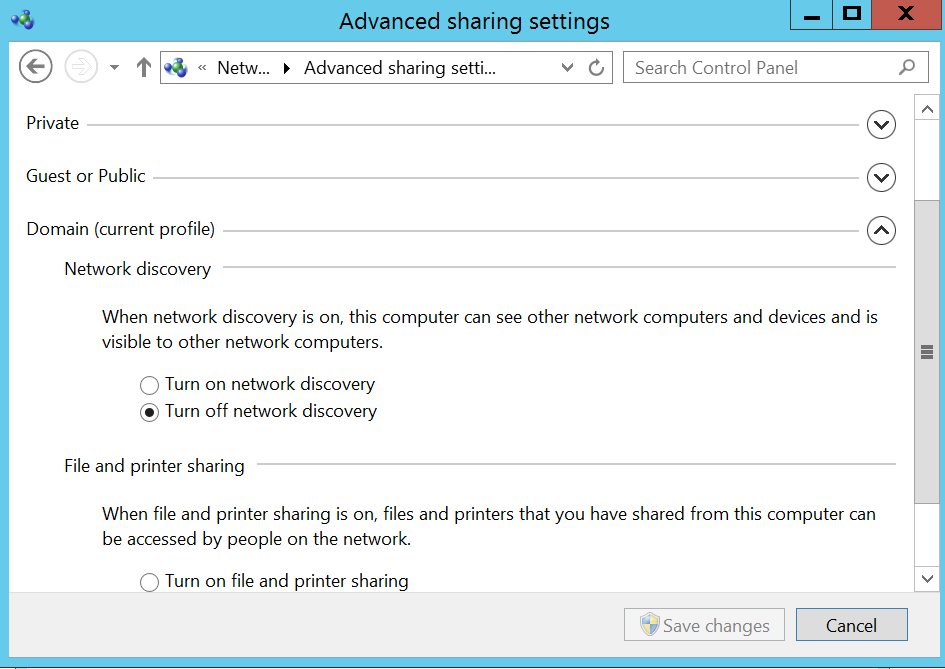


Reflection prompt: Do you understand the rules for effective permissions resolution when an account is receiving different set of permissions from more than one groups against the same resource.

Deny takes precedence regardless of full control permissions

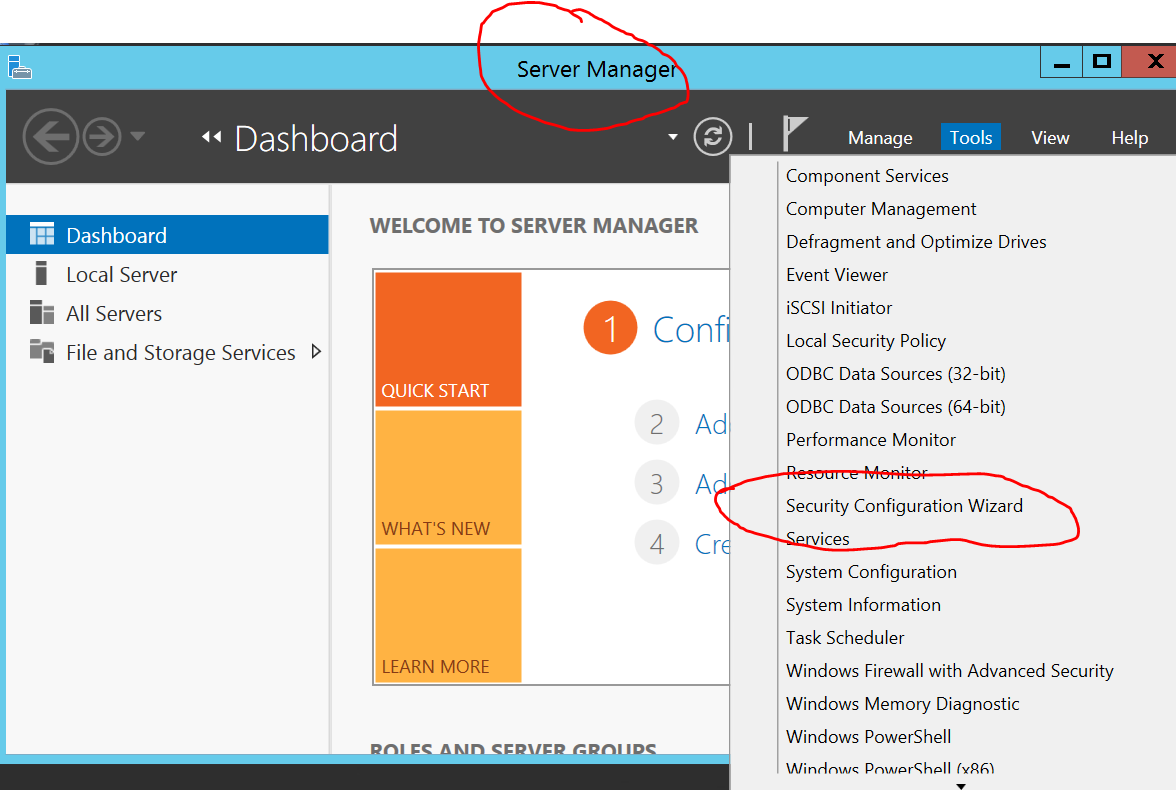
**Lab exercise 3-2a: Enabling the Shared Folder Feature.**

1. Login in as a Domain Admin to the Windows Server 2012R2
2. As Shared Folder feature requires to turn on the File and Printer Sharing and Network Discovery features at the server, you need to do that by getting into the Network and Sharing Center.
3. In the Network and Sharing Center, select Advanced sharing settings. You try to turn Network Discovery on. However, you can turn on the network discovery mode, but you cannot save the setting.
4. It is because the default network security settings, by default, disallows it to be turned on.

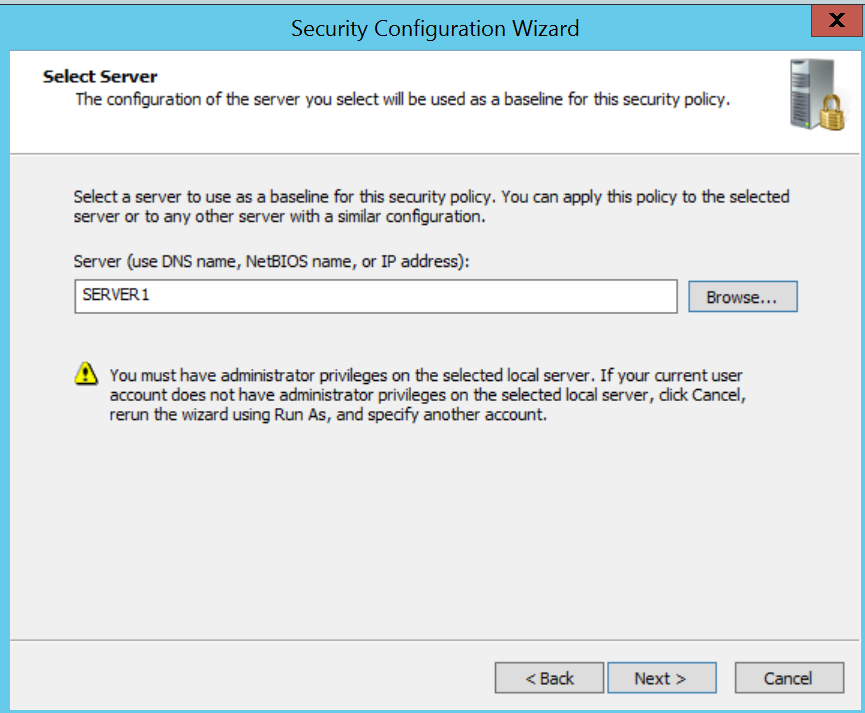


So how can we change the default network security rule? One way is to try to do it manually (update the firewall rules) , or we can use Security Configuration Wizard (SCW)\* to help, as described in the following steps:

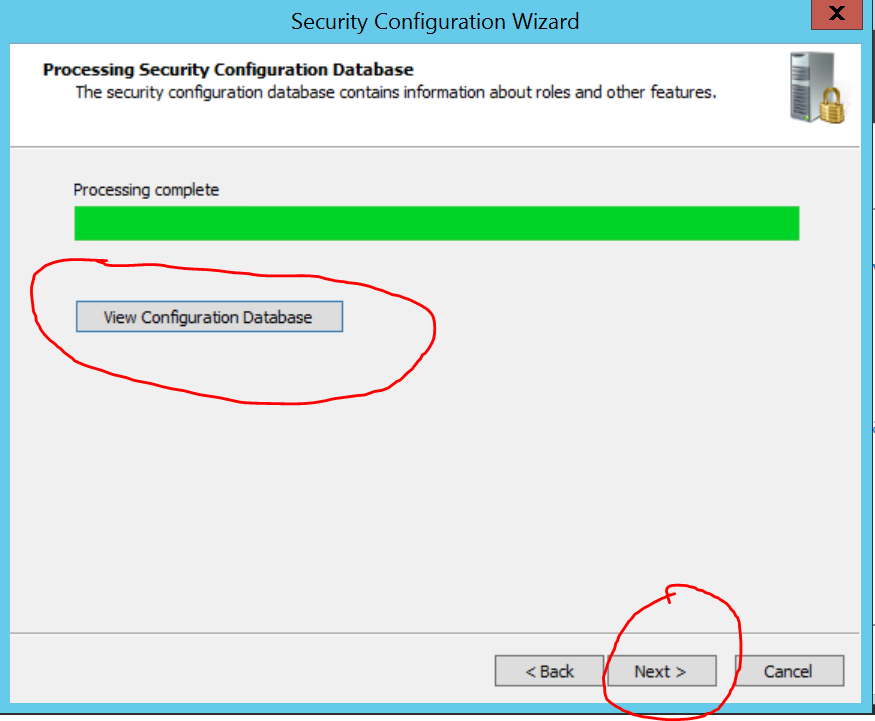
1. Run Security Configuration Wizard via the Tools menu of the Server Manager.



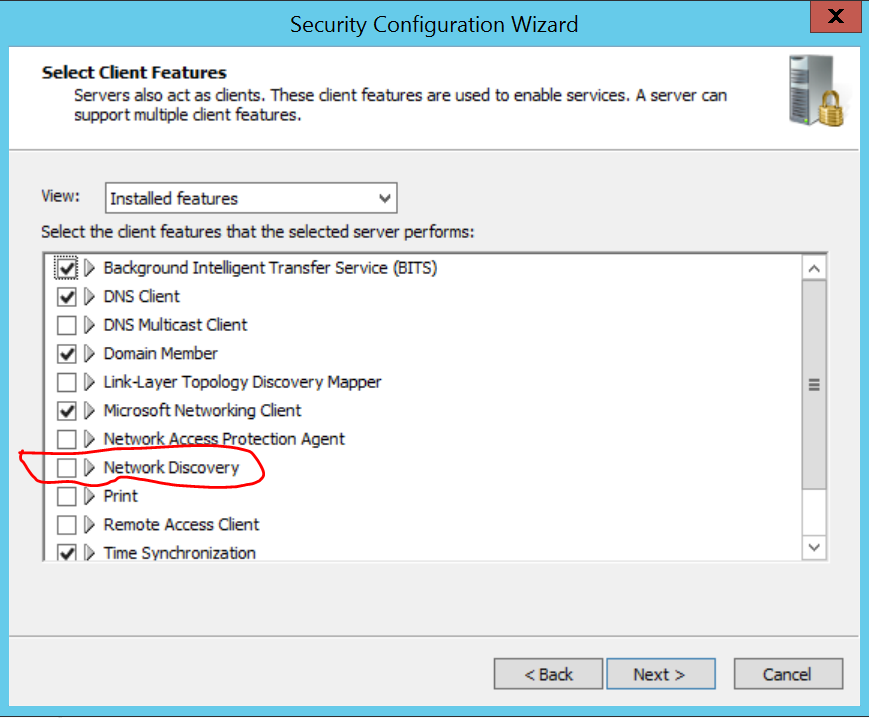
1. Use the default option of creating a new policy in the startup page. In the Select Server menu, simply choose your local Windows 2012R2 server (i.e. SCW will base on the installed roles of the target server to determine a recommended security configuration baseline.)



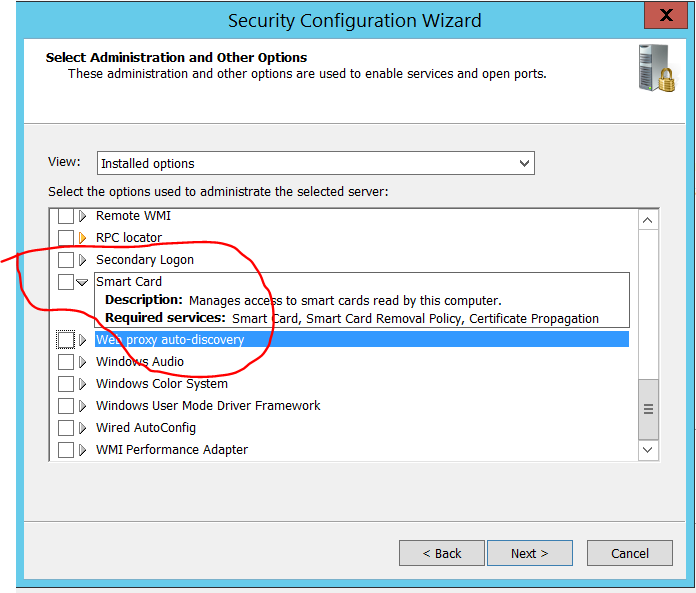
1. The next wizard screen will show you the processing status, since your windows server 2012R2 has not been added with any additional server role, the processing time should be very short. You may click on the ‘View Configuration Database’ button to bring up and view the build-in configuration rules and policy that the wizard is based on. (for your reading leisure) or you can press the ‘Next’ button to proceed.



1. In the subsequent screen, the wizard will show you the detected installed roles, features, options for your viewing and verification. (e.g. to discover unwanted features or missing of required option). In our case, we need to manually enable the ‘Network Discovery’ feature. You may press 'Next' to skip the 'installed roles' option page.



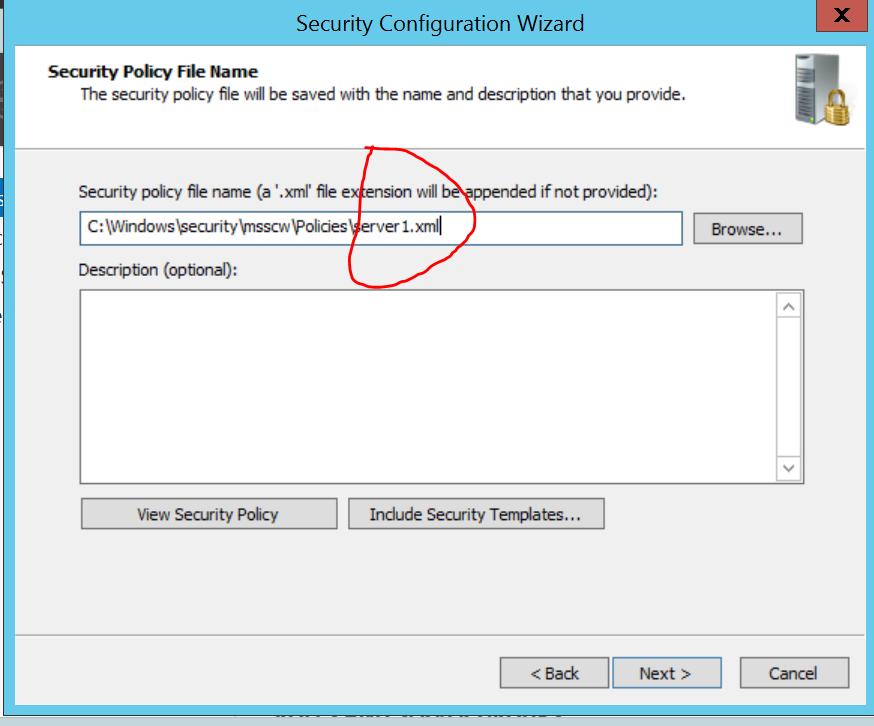
1. In the ‘Installed options’ screen, you may see the wizard has selected ‘Smart Card’ option for your server. Please ‘unselect’ it. The Smart Card option enables your server to be more ‘secured’ , however, since your system does not come with the smart card device, this option will just cause you login problem (Massive delay after you press the Ctrl-Alt-Del).



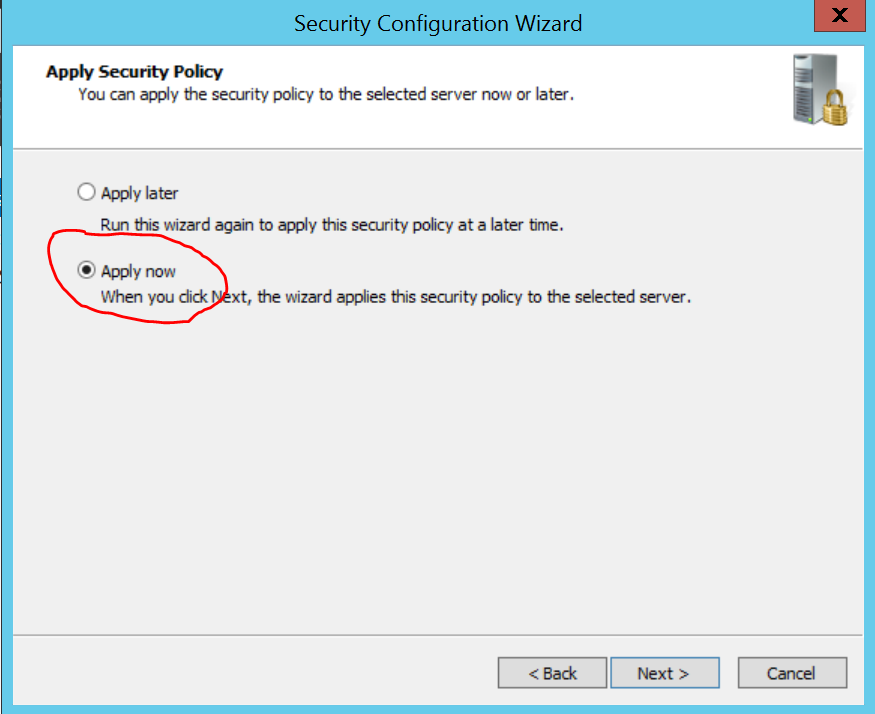
1. In the Confirm Services Change screen, take note of the wizard has suggested to change for all the listed services. (ie. For some services, they will be changed from Manual start to Disable and some others will be from Manual start to auto start.
2. When the wizard reaches to the Network Security Rules Screen, take note of that the wizard has enabled many network security rules (ie. Another way to refer to Firewall rules) based on the server role(s). Since you have selected the Network Discovery feature in the The File and Printer Sharing rules (actually enable network discovery)

# 

1. You can then go through the reminding wizard pages until the wizard prompt you to enter a file name for it to store the confirmed configurations. As you can see, you can use server1.xm as the file name.



1. In the next page, you will have the option to choose to apply the configuration later (the wizard only stores the suggested configuration in the named file) or apply the configuration immediately. In our case, you should choose apply now, in order to turn the Network Discovery on.



1. It will take some time for the wizard to apply the settings. (be patient).
2. The Network Discovery is related to the firewall settings, even the SCW has added in the required rules to enable the Network Discovery, you may need to restart the firewall services in order to enable the effect. Or you may restart your system to achieve the same effect.
3. Now go to the Network and Sharing Center again, to verify both of the Network Discovery and File Sharing features are turned on. (In case it is still not fully on, you may need to refer to [this](https://docs.microsoft.com/en-US/troubleshoot/windows-client/networking/cannot-turn-on-network-discovery) for a possible resolution.)

(ref: https://docs.microsoft.com/en-US/troubleshoot/windows-client/networking/cannot-turn-on-network-discovery)

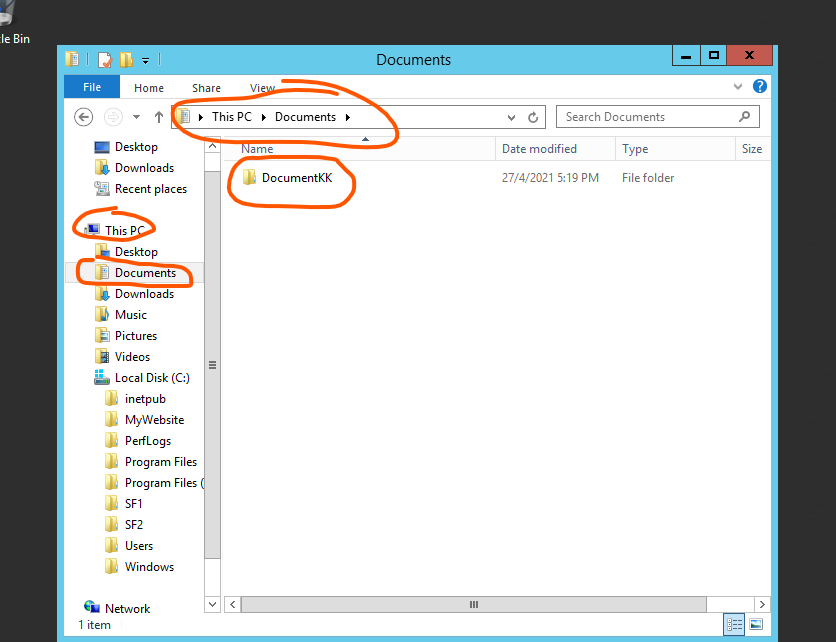
1. Refer to Activity 5-7 (Pg. 162) of the textbook for enabling sharing folder feature without using SCW.

\*SCW is a build-in Security Configuration utility for Windows Server Since Win Server 2008. It is easy to use, and it is a great tool to provide initial security hardening measure to a Windows Server. Microsoft has removed it from Win Server 2016. We can still find it in Win Server 2012 R2.

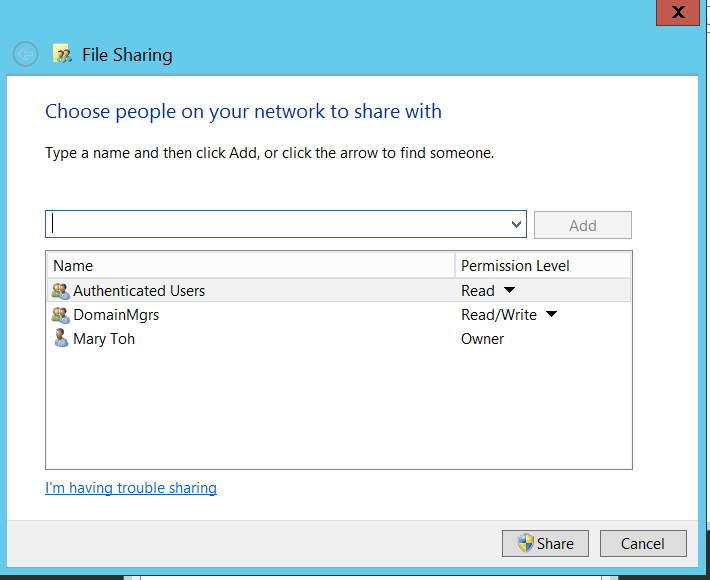
Caveat: At this point, you have completed a quick security hardening operation for your server. In the positive side, you have made your server much more 'secure'. One possible hiccup, however, you may encounter some issues in the subsequent SMW labs, as many default services of Server1 have been disabled by the SCW.

**Lab exercise 3-2b: Configuring a Shared Folder (Part 1) (STOP HERE)**

1. Refer to Activity 5-8 of the textbook to compete the requirement of the following exercise.
2. Login as the User1@yourDomain to the Windows Server 2012R2.
3. Navigate to This PC -> Documents and create a new folder with the name DocumentXX (XX is your initial).



1. Share out this folder and let DomainMgrs group members to have Read/Write Permission and Authenticated Users has Read Permission to this shared folder.

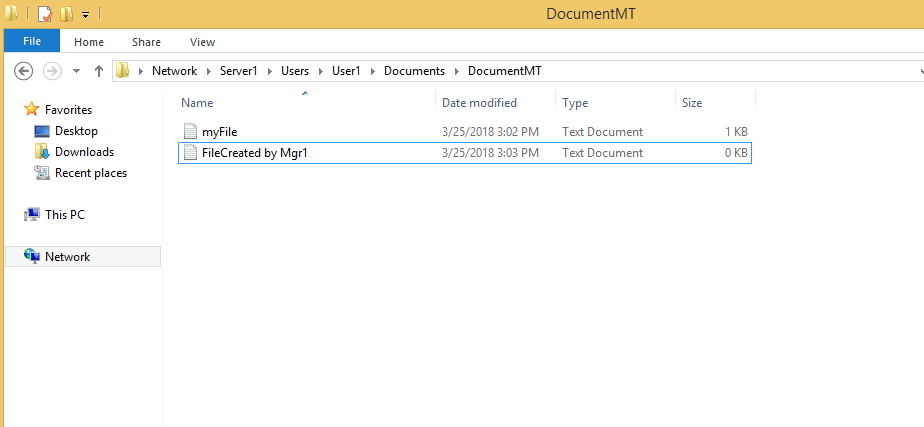


1. Click the Share button to complete the creation of the shared folder.

(You will be prompted for the Administrator credential to complete this sharing operation. Only administrators can create shares in a domain server.)

After you have shared out the folder, test your settings.

1. On Win 10, login as Mgr1.
2. Access the Shared folder. [\\*YourServer2012*/Users/User1/Documents\DocumentXX](file:///\\YourServer2012/Users/User1/Documents\DocumentXX) Test that Mgr1 can view, create and modify files in the shared folder (Mgr1 have Co-owner Share permission)



1. On Win 10, login as Staff1.
2. Access the Shared folder.
3. Test that Staff1 can view, but cannot make changes in the shared folder (Authenticated User has Reader Share permission only)

You can also view shared folders through the Network Node.

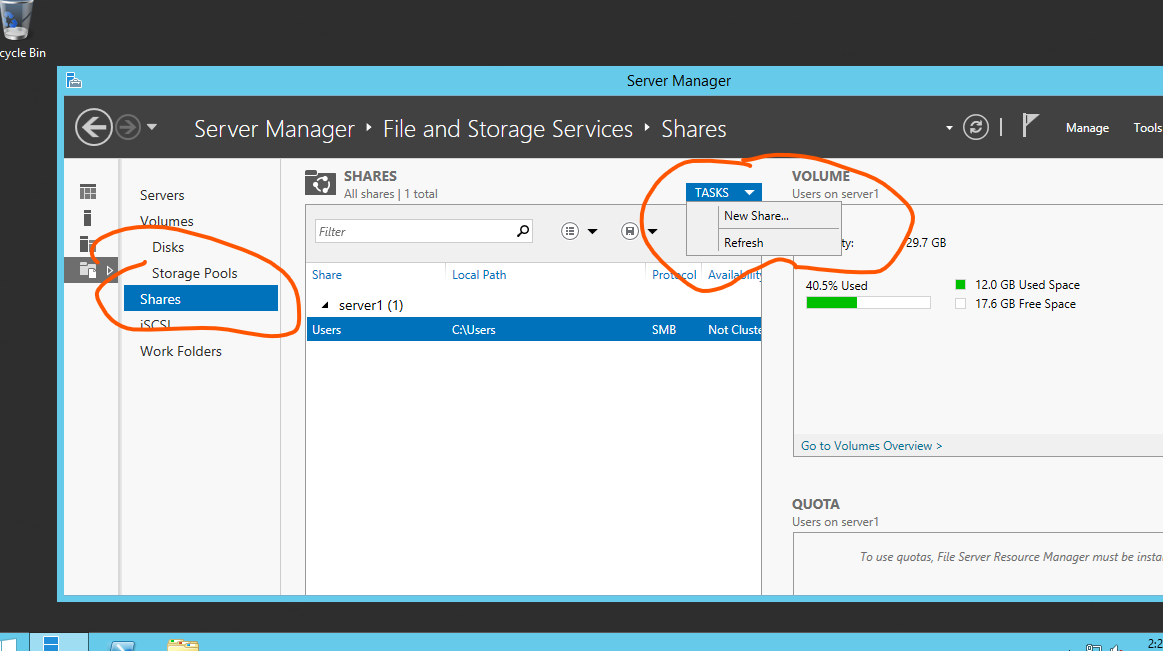
1. Go to Network (make sure Network Discovery is enabled on your Windows 10) and double-click on your Server2012R2 computer name.

**Lab exercise 3-2c: Configuring a Shared Folder (Part 2 - Using Server Manager)**

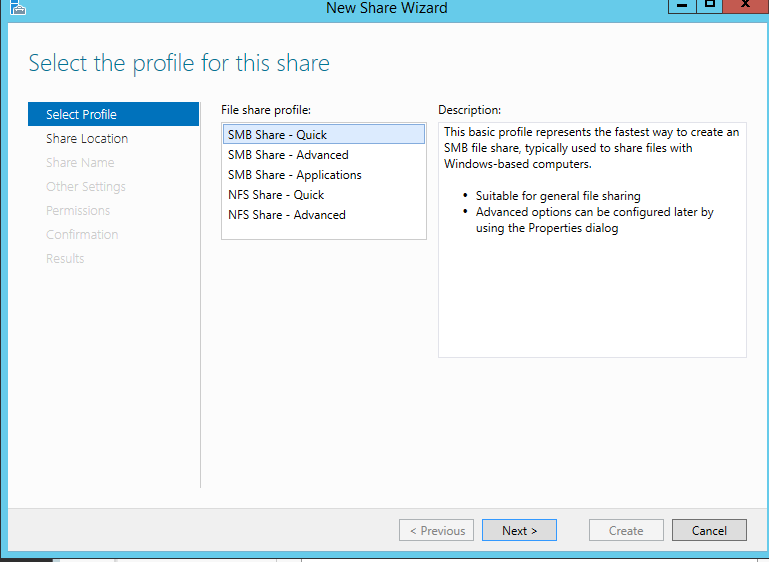
1. Refer to Activity 5-9 of the textbook for more information of the following exercise.
2. Login to your Server2012R2 with a domain admin account.
3. At the Server Manager, expand the File and Storage Services node at the left pane.

In powershell as administrator, go run winrm quickconfig and y to view shared file.

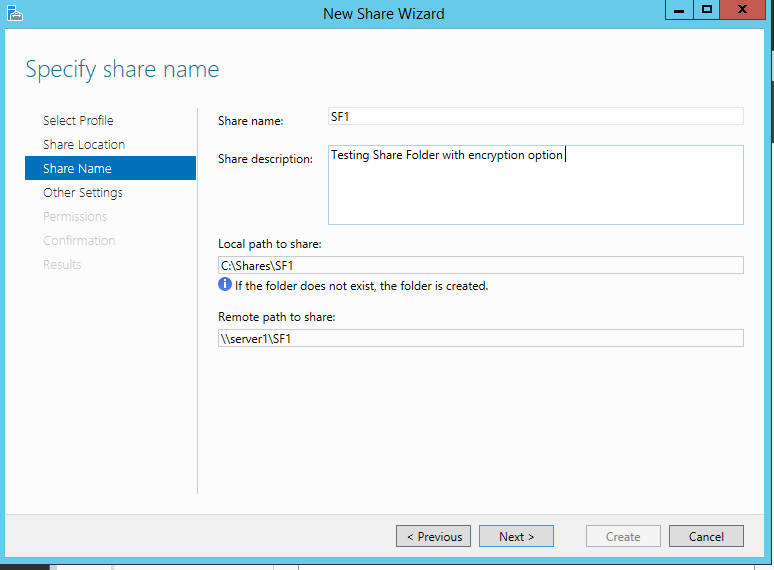
1. Click on the Shares node to bring up the monitor view of the existing Shares.



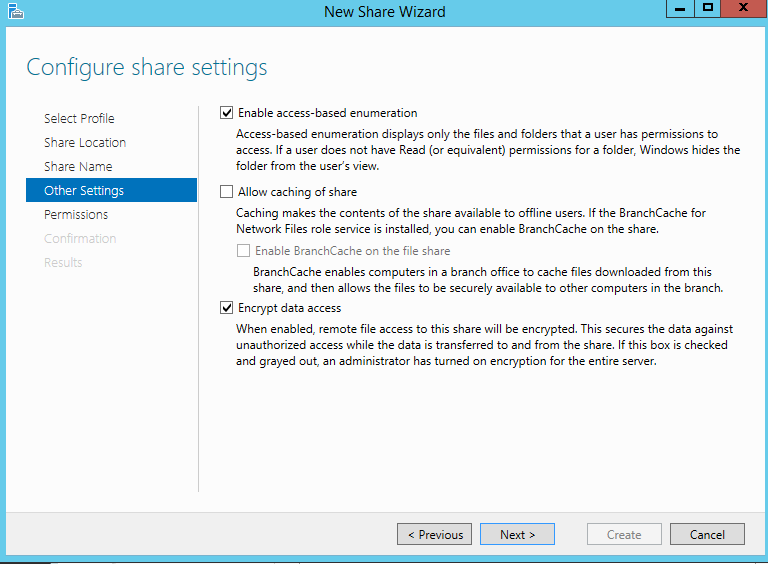
1. Click on the "New Share …" under the TASKS dropdown.
2. At Select Profile, choose SMB Share - Quick option, then click Next.



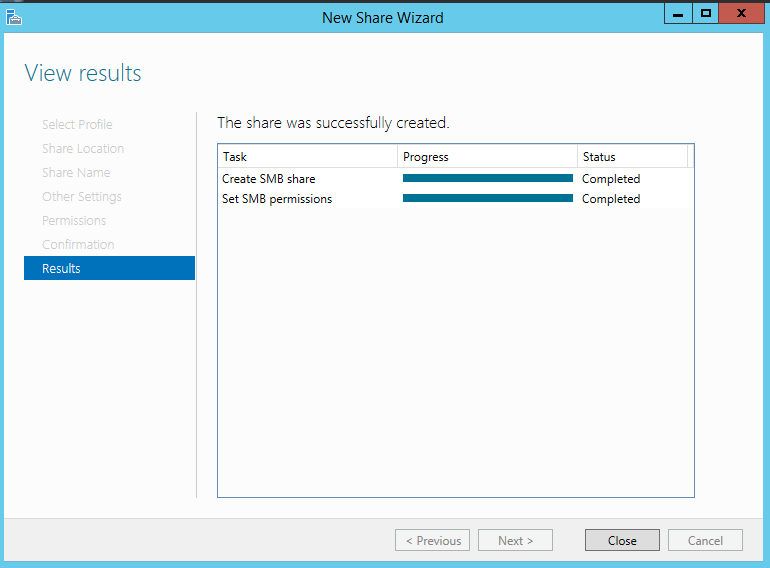
1. For share Location, you may take the default setting and press Next.
2. Enter the Share Name and Share Description in the Share Name View as shown:



1. At the next view, Other Settings, select 'Enable access-based enumeration' and 'Encrypt data access' settings.



1. Take all the default for the rest the views and create the new share 'SF1'.



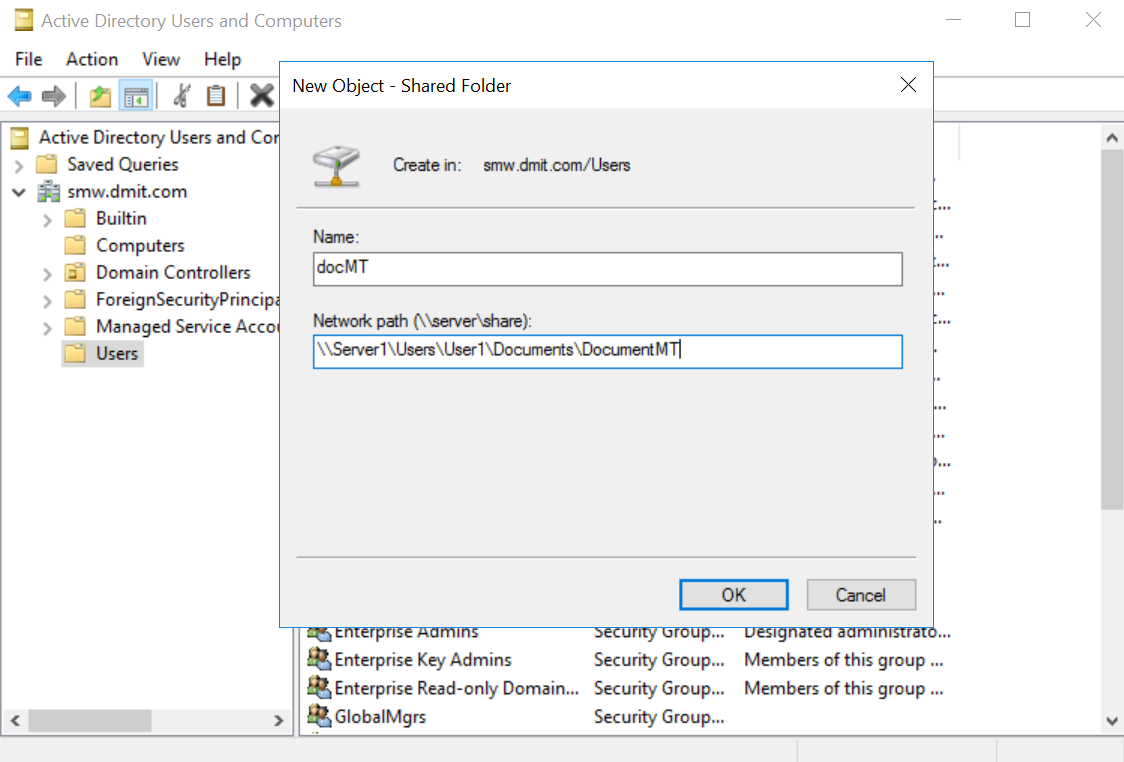
1. Explore a possible way to configure the permissions of the SF1: To let Mgr1 to have read/write access permission, and all domain user has read access permission.
2. Verify which accounts can access to SF1 from the Windows 10 client.

Ye only Mgr1 can edit.

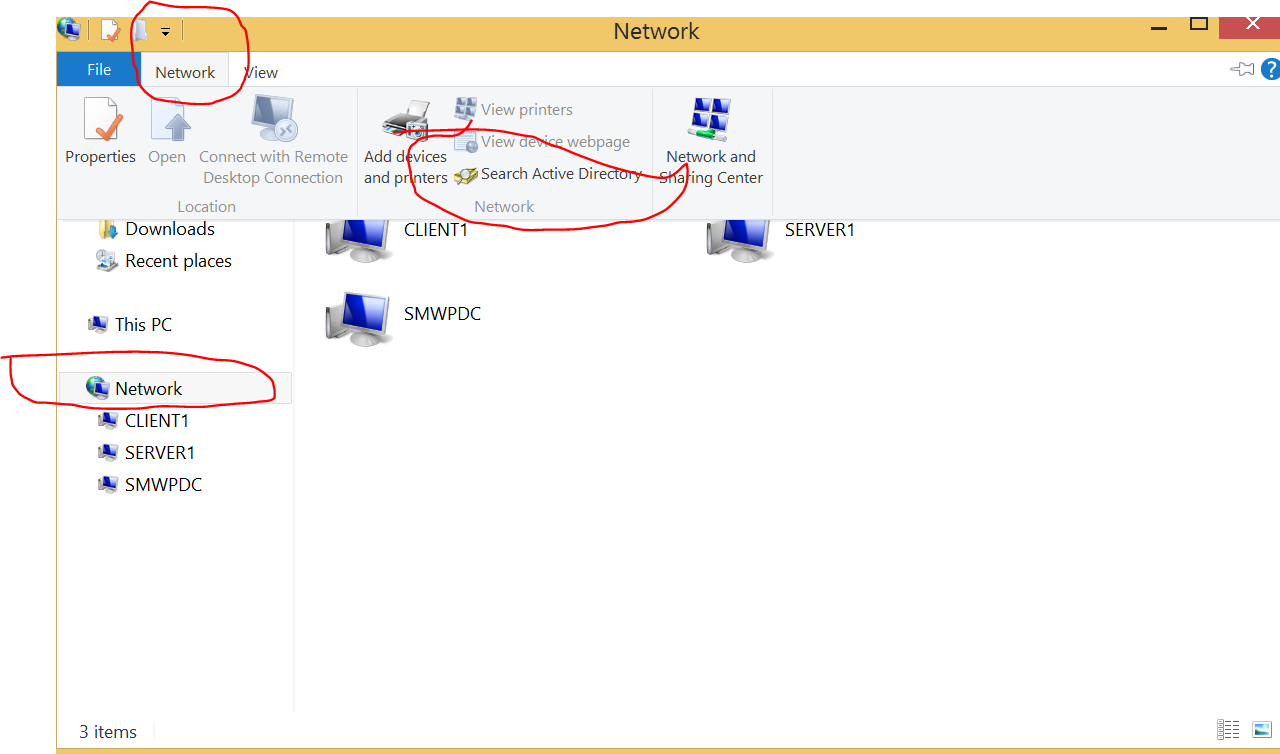
1. [Optional] Verify if the data transfer between the Windows 10 and the SF1 are encrypted (using the wireshark).

**Lab exercise 3-3: Publishing a Shared Folder**

1. Refer to Activity 5-10 of the textbook for this exercise.
2. The goal is to publish the shared folder(s) you have created in the previous exercises via the Active Directory.



1. In the Win 10, under the Network Node of the File Explorer, try to locate the shared folder via the



Reflection Prompt: Can you identify the Pros and Cons of the Publishing Shared Folder feature of the Active Directory?

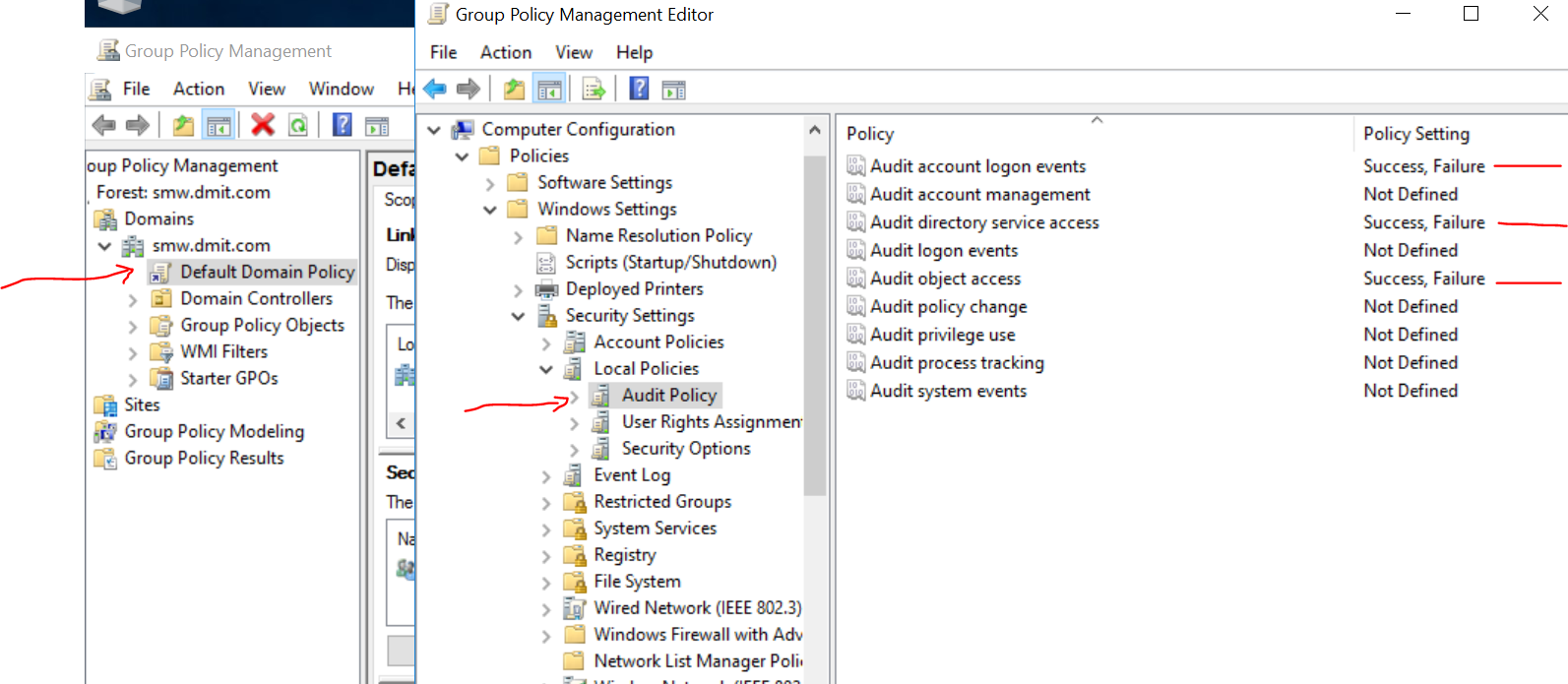
Pros: Easy to share to everyone within domain, OU or container

Cons:

**Lab exercise 3-4: Auditing a Login and Shared File Access.**

You will now audit failed logins and any access to the Shared Documentation folder/File.

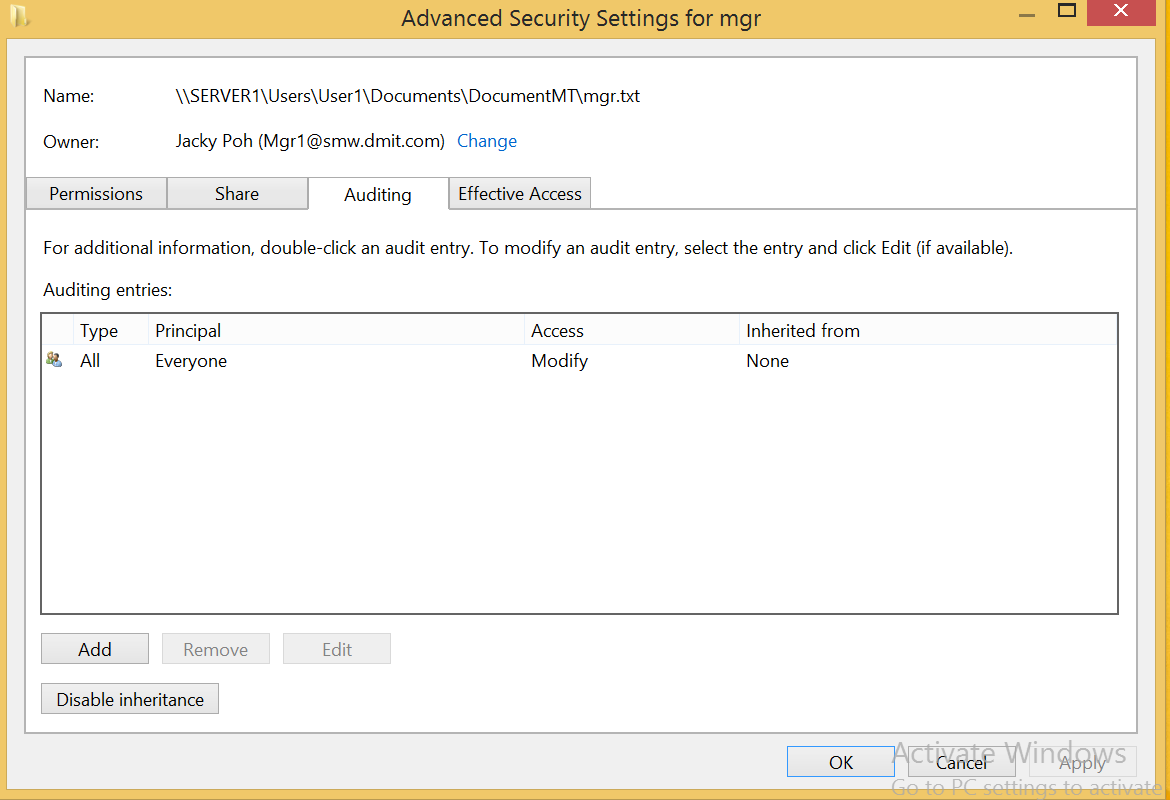
1. On the Domain Controller, login as Domain Administrator.
2. Refer to page 158 , Activity 5-6 Auditing a Folder for the steps to configure the Default Domain Policy to enable auditing for :
3. Audit directory service access - both SUCCESS and FAILURE
4. Audit object access - both SUCCESS and FAILURE
5. Audit account logon events - both SUCCESS and FAILURE



Note: In addition to turning on the Audit Success and Failure using the Group Policy, you need to set the audit option at the target object/folder/file explicitly.

1. Test your settings:

As Mgr1 on Win 10, access the shared folder created by User1 and create a new file “mgr.txt”. Enter some text in it. Ensure User1 have the read only access to this "mgr.txt" file. Set the audit option of “mgr.txt” to include both of the Success and Failure (via the Advanced Security Setting)-this operation requires admin right.



1. As Staff1 on Win 10, do a failed login (by using a wrong password) first. Then login with the correct password. Try open and read the mgr.txt from the shared folder. Try if Staff1 can update the content of the mgr.txt.

Staff1 can read but cant modify.

1. On Windows 2012R2, under Server Manager -> Tools, run Event Viewer.
2. Under Windows logs, Security, click on Find. Type “mgr.txt” to look for the logged event describing the access to the mgr.txt file. (you may double-click on the event and look at its Details).

Do you find the log events of Staff1 attempted to read (Success) and update (Failed) operation? No

(Hints: Open Event Viewer and search Security Log for event ID 4656 or 5145 with "Audit Failed" keyword, "File Server" or "Removable Storage" task category and with "Accesses: READ\_CONTROL" and Access Reasons: "WriteData (or AddFile) Not granted" strings. "Subject: Security ID" will show you who has tried to change a file.)

Please write down your finding here:

1. Click on Find again and type “Staff1” to look for the logged Audit Failure event describing his failed login.

Graphical user interface, application

Description automatically generated

**Lab exercise 3-5a: PowerShell for log tracing**

(This exercise should be done in your Domain Controller)

1. Refer to your text book and complete the Activity 3-14: Using Windows PowerShell (pg. 85).
   * Take note that the appendix B of the textbook also provides a list of PowerShell cmdlets
2. In PowerShell, type "get-help get-eventlog" to see a brief description for the get-eventlog cmdlet.
3. Type "get-help get-eventlog -full" to see a more detailed help screen.
4. Type "get-eventlog -list" to view the available event logs.
5. Type the following to list the events in the Application log which come from the source “VMTools”.

get-eventlog –logname application | where-object {$\_.source –eq "vmtools" }

1. Figure out how to use PowerShell to list the oldest 5 events in the Application log which come from the source of “VMTools”. ( hints: you may use the '|' pipe ,sort-object and select-object, to achieve that)

Reflection prompt: You may record down the commands that you have tried (and working).

**Lab exercise 3-5b: PowerShell for Domain Enumeration**

(This exercise is preferred to be done in your windows 2012R2 or Windows 10, strongly recommend using PowerShell ISH).

We will explore how to to collect Domain information using a domain user account. (no special administrative privilege.) via two approaches.

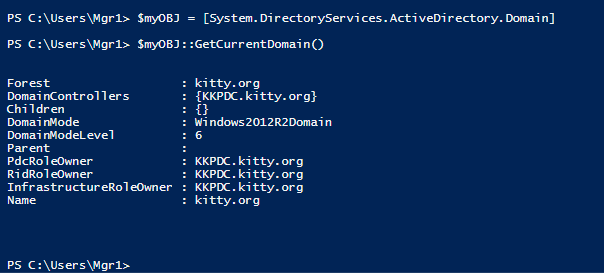
* Load in and Use .NET module at the PowerShell.
* Use cmdlets.

1. In Windows 10, login with as Mgr1
2. Search and open a PowerShell ISH session.
3. Create a Domain object with the following command at the ISH:

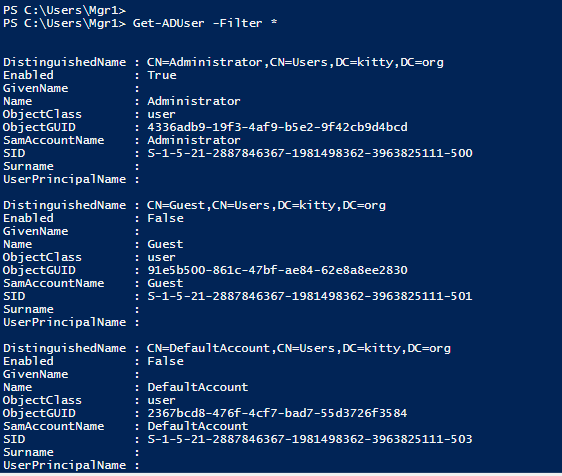
$myObj = [System.DirectoryServices.ActiveDirectory.Domain]

1. Execute the GetCurrentDomain() method to retrieve the domain information:

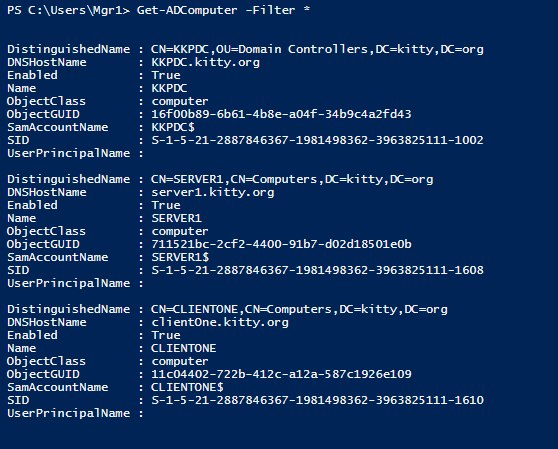
$myObj::GetCurrentDomain()



1. Execute Get-ADUser -Filter \* to retrieve a list of all the domain user accounts.



1. Execute Get-ADComputer -Filter \* to retrieve a list of all the domain computer objects.



**Lab exercise 3-6: View User Profiles**

1. In Windows 10, login with as domain or local administrator.
2. Go to C drive, Users folder.
3. Currently you will see that a folder has been created for every user that has logged in to the Windows 10 before.
4. In Windows Explorer, go to Organize, Folder and search options. Click on View. Choose “Show hidden files, folders and drives”. Uncheck “Hide extensions for known file types” and “Hide protected operating system files”.
5. You will now see more folders in the C:\Users folder, including the Default User folder and All Users folder.

The All Users profile hold settings for all users.

The Default User profile is used when a user first logs in. The Default User profile will be copied to a new folder with his username.

**Lab exercise 3-7: Set Roaming Profile [Optional] (STOP HERE)**

You will now set a roaming profile for Mgr1. A roaming profile means Mgr1 will have the same desktop settings on every computer he logs in the domain.

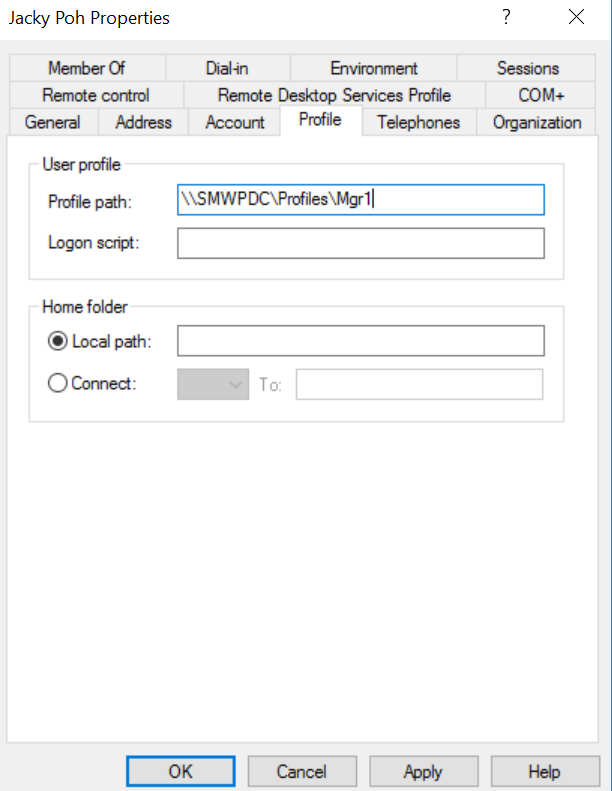
\*Assumption: The name of your domain controller is ‘SMWPDC’ , or else you have to use your own name when following some of the instructions.

First create a folder and share it out to the group Authenticated Users with Full Control :

1. On the Domain Controller, login with as domain administrator
2. Create a folder C:\Profiles
3. Right-click on Profiles and choose Properties.
4. Select Share tab. Click Advanced Sharing.
5. In Advanced Sharing, check the box “Share this folder.”
6. Click on Permissions. Click Add.
7. Type “Authenticated Users” and click Check Names. Click OK.
8. Give Authenticated Users the Share Permission of Full Control. Click OK.
9. Click OK. Click Close.

Now set a roaming profile for Mgr1 :

1. In Active Directory Users and Computers, right-click on Mgr1 and choose Properties.
2. Click on the Profile tab.
3. Set profile path to \\SMWPDC\Profiles\%username%. (see following diagram)



\*Note: you may need to substitute 'SMWPDC' with the name of your domain controller.

1. Click OK.

Test the roaming profile :

1. Log in to Windows 10 as Mgr1. Make some changes to the Desktop, eg create a folder on the Desktop and change the wallpaper. Log off (If you do not log off, the profile will not be updated to the server).
2. On Windows Server 2016, log in as Mgr1. You should see the same Desktop as on the Windows 10.
3. Look in C:\Profiles at the Domain Controller. A new folder Mgr1.v6 has been created, containing Mgr1’s user roaming profile. A”v6” is appended to the user’s name because Windows Server 2016 and Windows 10 use a user profile format version 6. Older versions of Windows are based on earlier versions, for example, Windows Server 2012R2 and Windows 8 are using version 2.

Reflection Prompt: In your view, do you think roaming profiles can be used to enhance the security level of a windows system ? Do you think roaming profiles can work in a workgroup environment?

~ End of Practical 3~