**Secure Microsoft Windows**

**Practical 2**

**Introduction to the Best Practices Analyzer (BPA) and Active Directory Basics**

|  |
| --- |
| **Objectives:**  After completing this lab, you should be able to:   1. Perform basic window storage management operations. 2. Using the Best Practices Analyzer to check against the configuration of a window server. 3. Create and configure Organization Units within a Domain. 4. Carry out basic domain user account management. 5. Using Remote Server Administration Tools (RSAT) Apps at the Client Workstation. 6. Understand the basic operations of security groups operations. 7. Create Fine-Grained Password Policy with Active Directory Administrative Center |

Lab Prerequisites:

Completion of the Lab exercises on Practical 1.

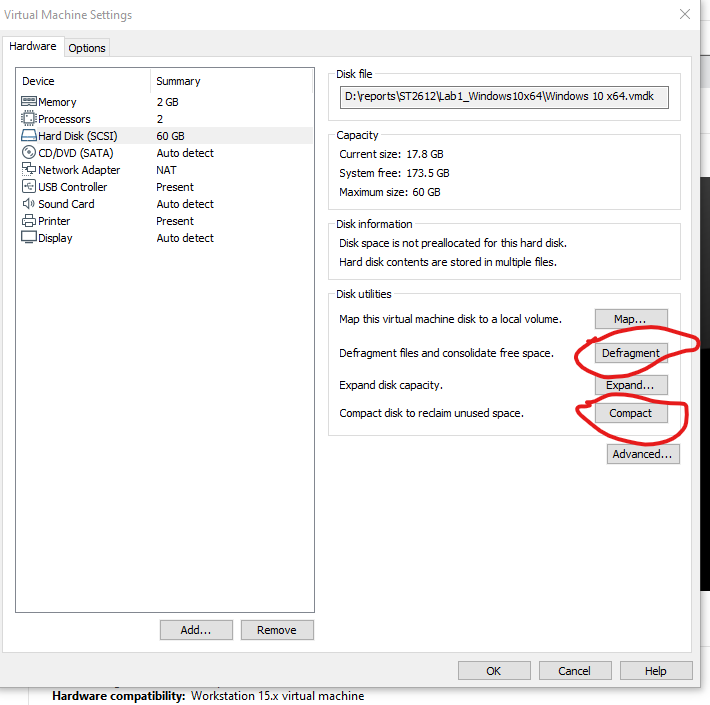
Have the basic understanding of Active Directory.

**Lab exercise 2-1: Adjust the virtual hard disk space on Windows 10 image**

1. Start up your Domain Controller first and then your Windows 10 image.
2. On your Windows 10, check how much free disk space you have on your C drive. If your free disk space is less than 10 GB, you would need to expand the hard disk in your image. Or you may want to reduce its size if you have more than 20GB free space. In other word, try to ensure the free space is at about 20GB or more level.

To expand/reclaim the hard disk space:

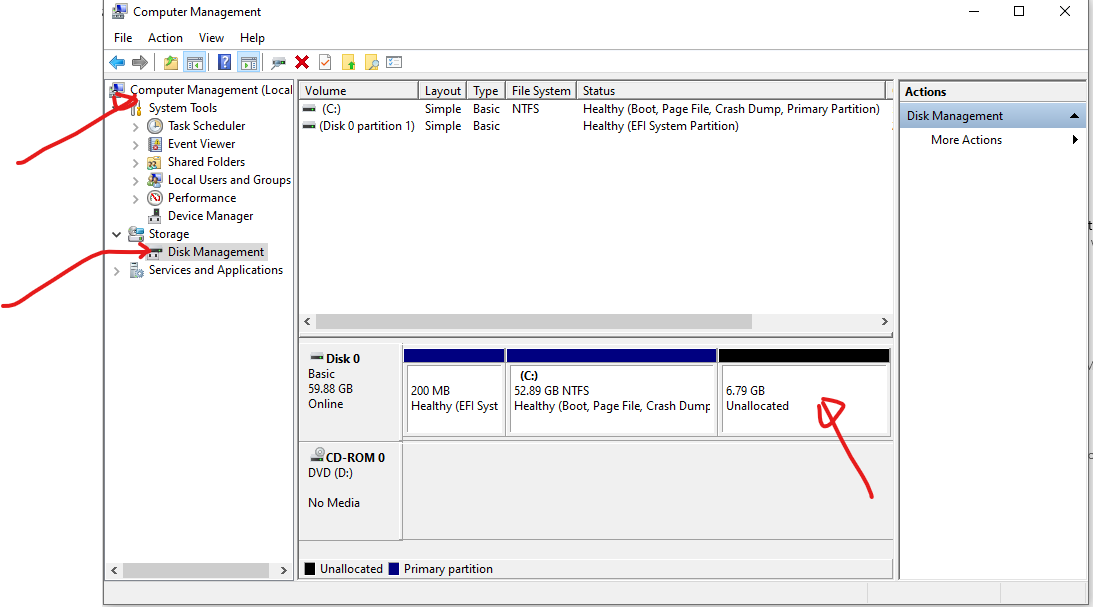
1. Shutdown your Windows 10 image.
2. Click on Edit virtual machine settings, and select 'Harddisk' to bring up the Disk Utilities menu. (on the lower right part)
3. Click the Defragment button (first) and the Compact button (second) to your tidy up your 'Harddisk' (Virtual) before proceeds to the following steps.



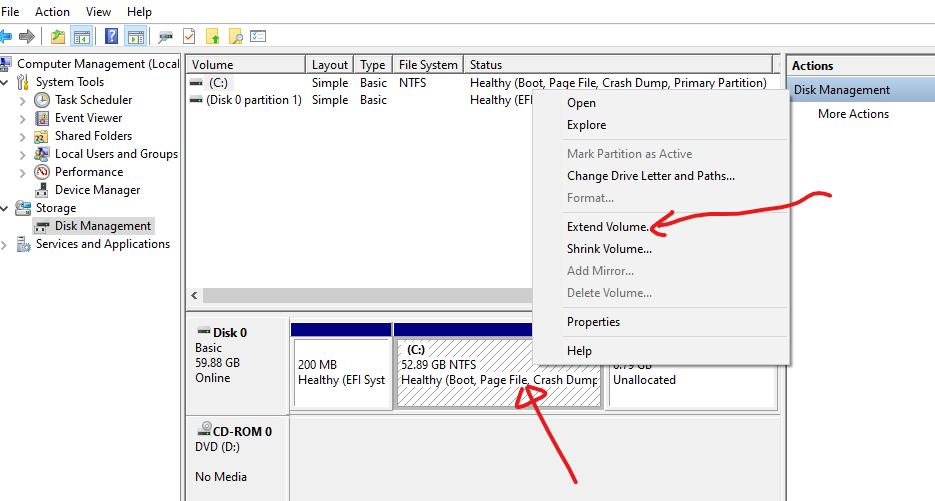
1. The above steps will help you to reclaim unused disk storages from the guest OS (The Windows 10) and return it to your physical machine (The host) .If you have enough free storage you may stop at this point. To increase the disk size, proceed with the following steps:
2. At the disk utilities panel, click the Expand button. Set the Maximum disk size to your target size. Click the Expand button at the bottom of the pop up menu to confirm.

(Take note that, due to the pre-allocated storage setting of your lab VM, this Expand option only allows you to increase the virtual disk size)

1. Power on the Windows 10 image.
2. Right click at the Start Icon, from the menu click on and bring up the Computer Management Console.
3. At the computer management console, under the Storage section , select Disk Management.



1. Right-click on the current disk partition and select Extend Volume. Extend the volume to use all the available disk space.

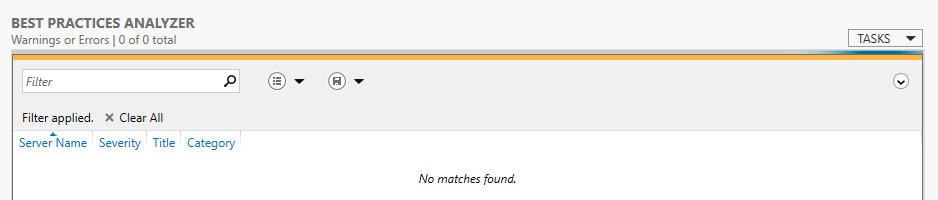


1. Close Computer Management.
2. Check and verify that the C drive now has more disk space.

Reflection Prompt: To adjust / expand the disk storage of a virtual machine is fairly easy. How about if you want to expand the disk storage of your physical notebook?

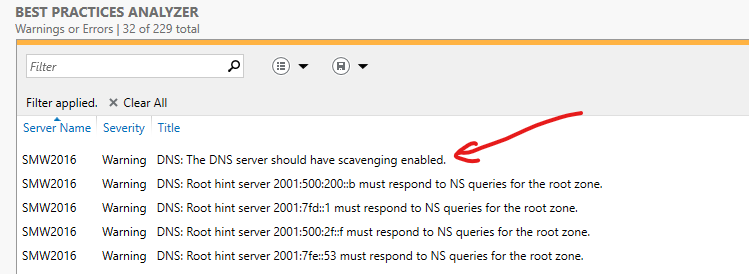
Add more ssds

**Lab exercise 2-2: Using Best Practices Analyzer (BPA) to check against your Domain Controller**

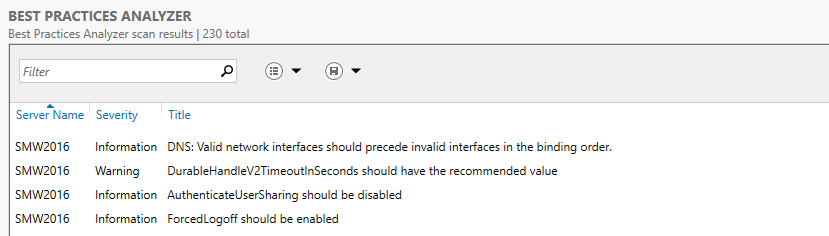


1. Login to your Domain Controller
2. Refer to Chapter-2 (page 59) of the textbook to start the BPA scan.
3. Review the result of the scanning and try your best to fix the sited issues.

* Please spend some effort in this exercise (about 30 minutes. To fix at least one or two issues.



After resolved the first warning issue and rerun the process, the report shown:



Reflection Prompt: How many issues the BPA has reported? How many of them have been fixed by you? Don’t need to be too worry if there are many issues that cannot be fixed.

217 BPA

Fixed 1 on DNS: The DNS server should have scavenging enabled

1. Take note of the BPA scanning is based on different sets of rules:

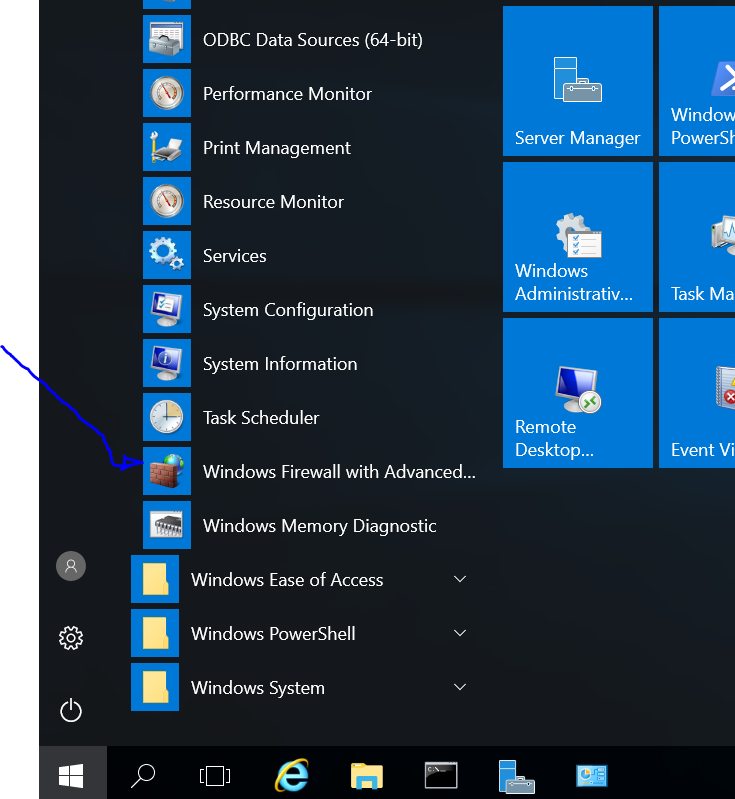
The following table describes the best practice rules categories against which roles are measured during a Best Practices Analyzer scan.

| **Category Name** | **Description** |
| --- | --- |
| Security | Security rules are applied to measure a role's relative risk for exposure to threats such as unauthorized or malicious users, or loss or theft of confidential or proprietary data. |
| Performance | Performance rules are applied to measure a role's ability to process requests and perform its prescribed duties in the enterprise within expected periods of time given the role's workload. |
| Configuration | Configuration rules are applied to identify role settings that might require modification for the role to perform optimally. Configuration rules can help prevent conflicts in settings that can result in error messages or prevent the role from performing its prescribed duties in an enterprise. |
| Policy | Policy rules are applied to identify Group Policy or Windows registry settings that might require modification for a role to operate optimally and securely. |
| Operation | Operation rules are applied to identify possible failures of a role to perform prescribed tasks in the enterprise. |
| Predeployment | Predeployment rules are applied before an installed role is deployed in the enterprise. They let administrators evaluate, before the role is used in production, whether best practices were satisfied. |
| Postdeployment | Postdeployment rules are applied after all required services have started for a role, and after the role is running in the enterprise. |
| Prerequisites | Prerequisite rules explain configuration settings, policy settings, and features that are required for a role before BPA can apply specific rules from other categories. A prerequisite in scan results indicates that an incorrect setting, a missing program, an incorrectly enabled or disabled policy, a registry key setting, or other configuration has prevented BPA from applying one or more rules during a scan. A prerequisite result does not imply compliance or noncompliance. It means that a rule could not be applied, and is not therefore part of the scan results. |

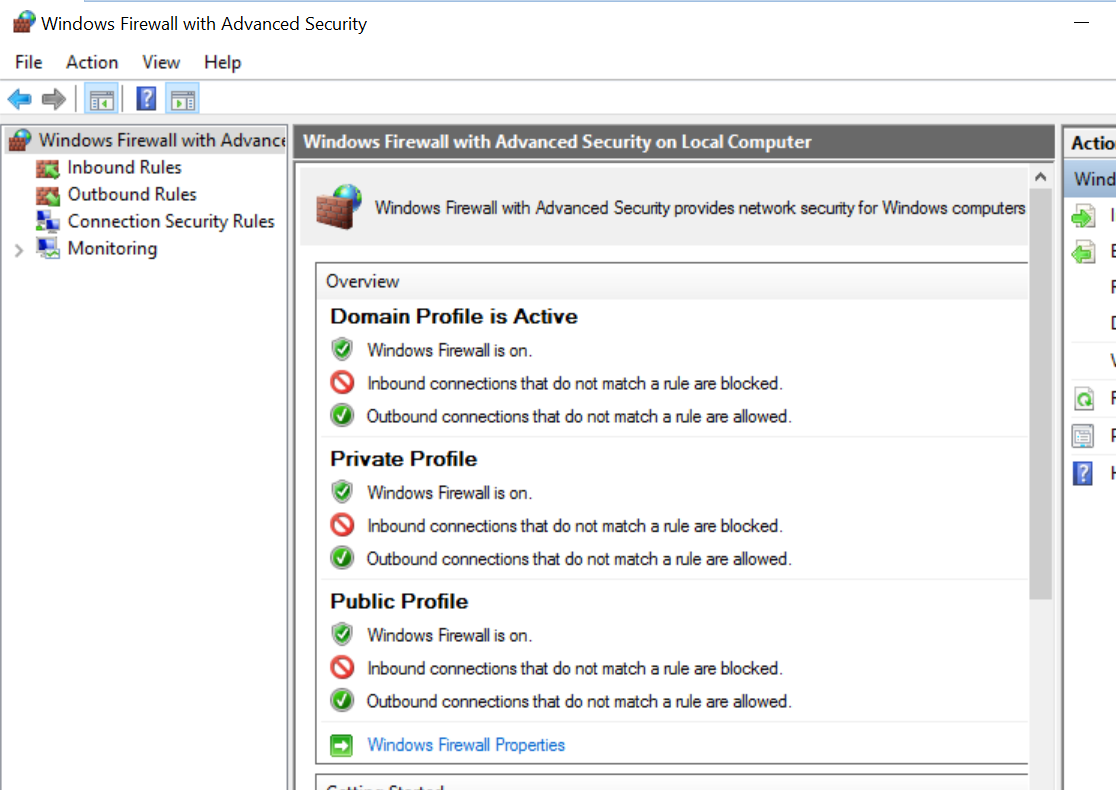
~Reference: https://docs.microsoft.com/en-us/windows-server/administration/server-manager/run-best-practices-analyzer-scans-and-manage-scan-results

**Lab exercise 2-3: Viewing Firewall Rules** (At your Domain Controller)

1. Left click the Windows button, expand the Windows Administrative Tools, and click on the Windows Firewall with Advanced Security.



1. Look at the Overview pane. Which Firewall profile is currently active?



Reflection Prompt: Do a quick self-research and figure out what is the purpose of these 3 Profiles for? And identify the unique different attributes of Domain Profile and Private Profile.

1. Click on Inbound Rules. Can you find the rules that allow clients to connect to your DNS Server? Which ports is the DNS Service running on? Is there any restriction on which client IP address can connect to your DNS Server?

Port 53

1. Can you find the rule that allows other systems to ping your Windows Server 2008?

File and Printer Sharing (Echo Request - ICMPv4-In)

**Lab exercise 2-4: Raising the Forest and Domain Functional Level**

In the previous practical, you had set the Domain Functional Level to Windows Server 2008. You will now raise it to Windows Server 2012 R2. (You can raise the Functional Level but you cannot lower it after that)

1. Refer to the chapter 3 (Page 104 - 105 and Figure 4-11) of the textbook for the step by step instructions of this exercise.
2. Refer to the chapter 3 (Page 108 , Activity 4-2) of the textbook to verify the Domain Functional Level has also been updated to Windows Server 2012 R2.

Reflection Prompt: Search and discuss with your classmates to figure out why windows provides this Raising Domain Functional Level feature?

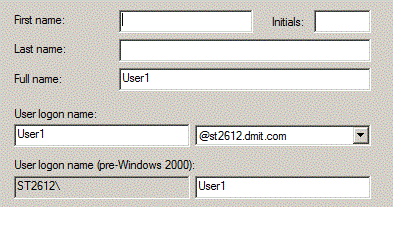
To update servers?

**Lab exercise 2-5: Creating Domain User Accounts in Active Directory**

You will now proceed to create THREE domain user accounts on your Domain Controller. Domain users are able to login to any computer in the domain, except for the domain controller.

1. Refer to the chapter 3, Activity 4-4 of the textbook for the step by step instructions of this exercise with the following additional requirement:

* Give your 3 users the following Full Names and User logon names: User1, Staff1 and Mgr1



* For passwords, you can use: 1qwer$#@!

\*Note- the above screen shot is based on the domain of st2612.com, it may be different from your actual setup.

1. Start up your Windows 10 image. Click on Switch User. Login as one of the 3 domain user accounts you just created. When asked to change password, you can use !QWER4321.

Reflection Prompt: We usually consider it is a good practice to ask a user to change his password upon the first successful logon session. Why is it so?

**Lab exercise 2-6: Group Policy controlling access to the Domain Controller**

As the Domain Controller is a very important server, physical access to it should be restricted. Moreover, direct logon to the Domain Controller should also be restricted. In fact, by default, there is only a handful of user accounts are allowed to do so.

1. On the Domain Controller, try to login as any one of the 3 domain user accounts just created. You should not be successful. (This an example of security by default!)
2. Login as the Domain Administrator.
3. Under Administrative Tools, run Group Policy Management. Expand your domain. Under Domain Controllers, there is a Default Domain Controller Policy. This is the policy that controls all Domain Controllers in your domain. (Note: do not mistakenly select the Default Domain Policy instead)
4. Right-click on Default Domain Controller Policy and select Edit.
5. Expand Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies. Click on User Rights Assignments.
6. In the right-hand pane, double-click on Allow log on locally. Are normal users among the groups who are allowed to log on locally on Domain Controllers? NO
7. Click on Add User or Group. Click Browse.
8. Type “Mgr1” and click Check Names. Click OK. Click OK. Click OK.
9. Try to login as Mgr1 on the Domain Controller. You should be successful now.

**Lab exercise 2-7: Granting Administrative Rights to user account by security group member**

1. Create another domain user account (give any name you like) and make him/her a member of the Domain Administrators group.
2. Try to use the newly created account to logon to the domain controller directly to prove it has the administrative right.

Reflection Prompt: Can you suggest any additional ways to prove the new account has the domain administrative right?

Check user properties under member of

**Challenging Task (Optional)**

Create and apply ascript/programto create 200 user accounts in your domain.Suggested logon name patterns (User201 to User400), suggested password patterns (p@ssw0rd201 to p@ssw0rd400) [Hints: check out the usages of dsadd and dsquery commands]

**If you are successful, post your script to the BB to share and compare with others.**

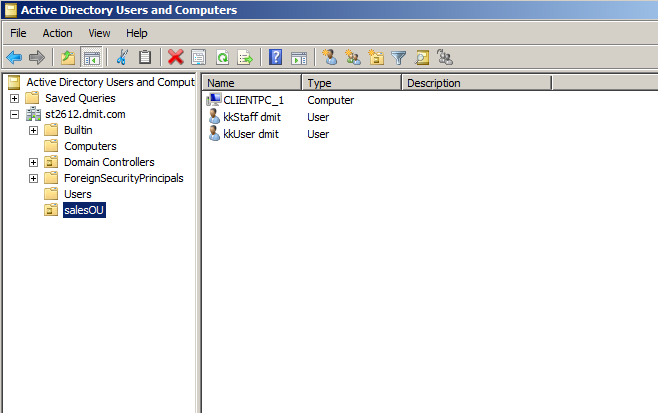
**Lab exercise 2-8: Managing Organizational Units (OU) ( STOP HERE )**

1. On your Domain Controller, refer to the chapter 3 , Activity 4-3 of the textbook for the step by step instructions of this exercise with the following additional requirement:

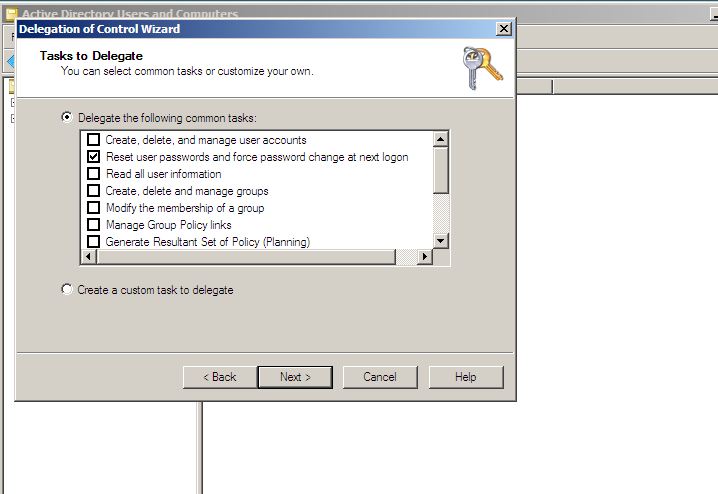
- Create a new OU (Organization Unit) called SalesOU to your domain.

- Move the following Directory Objects into this salesOU

The User1 and Staff1 user account objects, and your Windows 10 computer object. Click Yes if you see a warning message about moving objects in Active Directory.



- Try out the delegate control wizard at SalesOU. Delegate the control of SalesOU to the Mgr1 account (only with Reset user passwords and force password change at next logon control)



The above should enable the Mgr1 to reset passwords for users who are in the Sales OU.

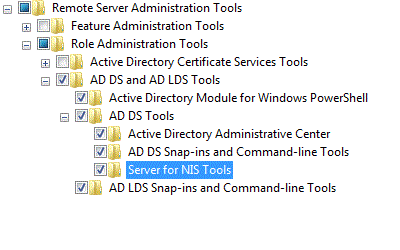
Please carry out a quick test to verify it.

**Lab exercise 2-9 Installing/Configuring Server Administration Tools on Windows 10**

It is often that the Administrators may wish to carry out admin tasks like creating domain users using their own workstations, instead of having to physically go to the Domain Controller every time. They can install Remote Server Administration Tools (RSAT) on to their own workstations (running windows 7/8/8.1/10). Prior to Windows 10 RSAT was required to download and install separately to the client system. For Windows 10, RSAT is prepared as an 'APP' in the system.

For Windows 8.1 or older version of clients

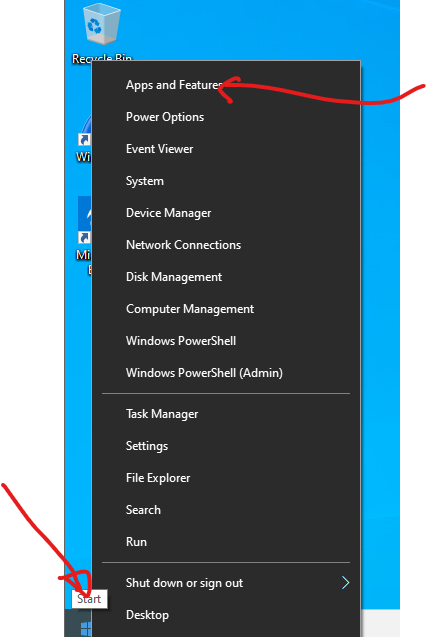
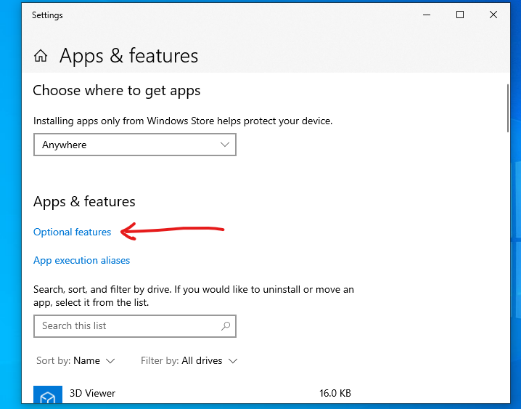
1. For Win 8.1 or older version of clients, you may need to search on the Internet for “Remote Server Administration Tools for Windows” that matches your need and download it.
2. After downloading, check how much free hard disk space you have left on the image. You need to at least 5 GB free space in order to proceed for the installation.
3. In case you have insufficient space, you have to expand the virtual hard disk space on Windows image (Please refers to Lab exercise 2-1)
4. Install the downloaded Remote Server Administration Tools (RSAT) to your client workstation. (Note: This may take twenty minutes! It is because the installation adds updates into the Windows Systems RSAT tools are features of the systems rather than an add-on application.)
5. Special note: By default, RSAT is enabled after the installation in windows 8.1.
6. Below (up to step 13) is an example of how to enable/disable the related features in your workstation. Click Start, click Control Panel, and then click Programs.
7. In the Programs and Features area, click Turn Windows features on or off.
8. If you are prompted by User Account Control to enable the Windows Features dialog box to open, click Continue.
9. In the Windows Features dialog box, expand Remote Server Administration Tools.
10. Expand Role Administration Tools.
11. Check everything under AD DS and LDS Tools (see following diagram).



1. Click OK.

For Windows 10:

1. Right Click on the Start button and click on the Apps and Features menu.



1. At the Apps and Features Popup, click on the Optional features link, you will find all the installable RSAT components.
2. At the top of the pop up, click on the Add a feature + button, you will be able to find and installed additional Apps.
3. Search for "RSAT" and you will see a list of RSAT relate Apps.
4. You should install RSAT: Group Policy Management Tools and RSAT: Active Directory Domain Services and Lightweight Directory Service Tools.
5. After the installation, logout and then Login as Mgr1 (Domain user account) at the client Windows workstation.
6. Search for and start Active Directory Users and Computers console from the RSAT.

Or

1. Go to Start, Run and type “mmc”. Go to File, Add Snap-in. Select Active Directory Users and Computers.
2. In Active Directory Users and Computers, expand your domain. Test if Mgr1 can reset the passwords of User1 and Staff1 (they should be in the SalesOU). In the previous exercise, you had delegated control to Mgr1 to be able to reset passwords of users in the SalesOU.
3. As Mgr1, try to move User1 back to the Users container. You should not be successful.
4. As Mgr1, try to reset the password of Administrator. You should not be successful.

Mgr1 can only reset passwords of users in the SalesOU.

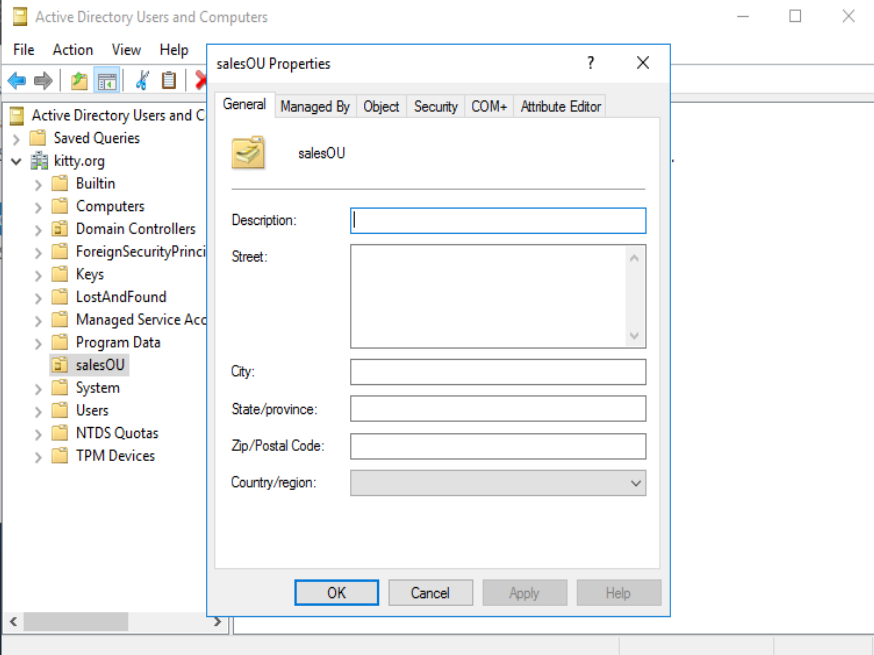
Reflection Prompt: Think about the delegation feature, what are the pros and cons of this features in terms of operations and system security?

Cannot revoke permissions or delegation to given account.

View and manage delegation setting via Advanced Security Settings menu [Optional]

In the previous section (Ex. 2-8), you have delegated the reset user password permissions to the user account 'Mgr1' for the salesOU. It has been accomplished via the Delegation of Control Wizard. To use the Wizard is easy but it only allow you to do a quick 'adding of permissions' to an user account. It does not allow you to revoke such permissions (or delegation)!

1. At the Active Directory Users and Computers view. Enable the 'Advanced Features' under the View menu.
2. Right click at the salesOU node and select the properties menu to open the salesOU Properties windows:



1. Click on the Security Tab and you can explore the 'Advanced Security Settings' of the salesOU object. You can also find out how the 'delegation of control' works with special permissions settings.
2. Close the Active Directory Users and Computers. You can save the Console1 if you wish to.

**Lab exercise 2-10 Create Local User Accounts to login to one system only**

There may be occasions when you just need to create a local user account for logging in to just one system.

1. Login to your client Windows image using an administrator account (local or domain).
2. Go to Administrative Tools, Computer Management.
3. Under System Tools, expand Local Users and Groups. Click on Users.
4. In the right hand pane, right-click and choose New User.
5. Enter a User name and the password. Click Close.

Reflection Prompt: Think about the difference between the domain user accounts and local user accounts, and the reasons that to have these two types of user accounts.

**Lab exercise 2-11 Create Domain Local and Global Security Groups**

1. Login as the Domain Administrator on
   * your client Windows image.
   * Or your Domain Controller (if your RSAT tools are not working in your client Windows workstation.)
2. Run Active Directory Users and Computers console (or you may try to run mmc and add the Snap-in).
3. Create a Domain Local Group: DomainMgrs and a Global Security Group: GlobalMgrs-

Refer to Activity 4-9 of the textbook for the step by step instructions to complete this exercise.

* + For Step 17, select only one the user accounts Mgr1.
  + For Step 19, verify that only Mgr1 is in the Member tab of the GlobalMgrs group.
  + Note: You need to use the DomainMgrs and GlobalMgrs security groups created in this exercise in the next practical exercise.

**Lab exercise 2-12 Fine-Grained Password Policies and Active Directory Administrative Center**

Fine-Grained Password Policies (FGPP) allow you to create multiple password policies for specific users or groups. Multiple password policies are available starting with the Windows Server 2008 version of Active Directory. In previous versions of AD, you could create only one password policy per domain (using the Default Domain Policy).

Administrators can create multiple FGPPs in Password Setting Objects (PSO). Individual PSO can be associated to a **global** security group to set the password policy requirement for the members of the group.

There are different ways to create the PSO. In this exercise, you will explore and use the Active Directory Administrative Center (ADAC) to create a testing PSO and associate it with GlobalMgrs security group.

For this testing PSO, you can set the password requirements (length=6, complexity=No, history=3) and account lockout option = None.

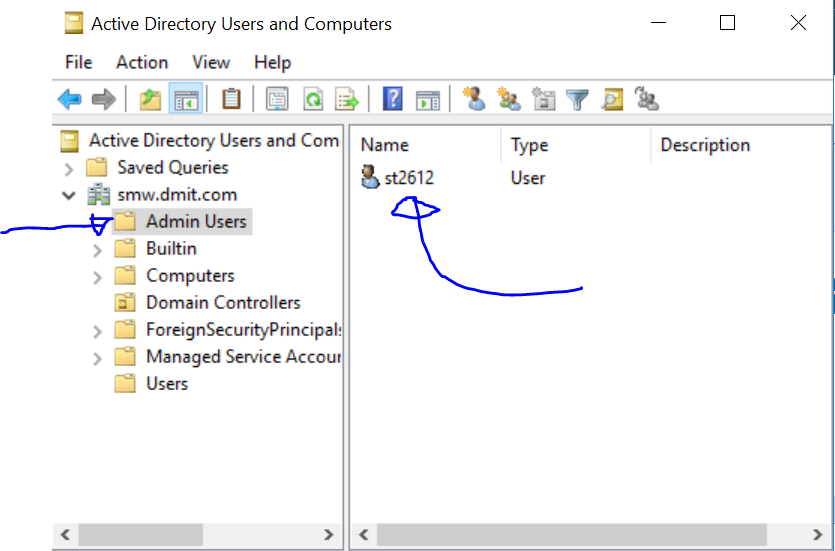
Please refer to the following video for the usage of ADAC to accomplish the task.

[*"How To Manage Fine-Grained Password Policies In Active Directory"*](https://www.youtube.com/watch?v=7AZGuUBin9U)

Verify your configuration with the Mgr1 account, that is: Log in as Mgr1 and try to change the password.

**Challenging Task (Optional)**

Create a new container (This feature, by default, is hidden) in your domain with the name ‘Admin Users’. You can then move the st2612 user account from the default container (User) to you newly created Admin Users container.



Hints: To enable the container creation, you need to use the Active Directory® Service Interfaces Editor (ADSI Edit) Admin tool.

**If you are successful, show it to your tutor.**

1ST step: Add acc to “Schema Admins” security group

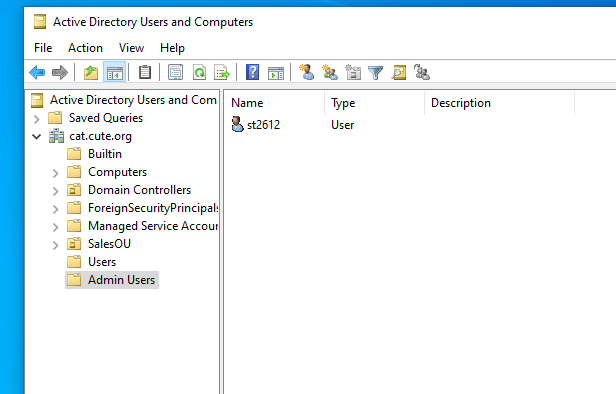
Restart pc

With new permissions, go to ASDI edit, right-click -> connect to and select schema

Then go to CN=Container properties

Set defaultHidingValue as FALSE (was set as TRUE)

<https://robinhobo.com/how-to-create-container-objects-in-active-directory-not-ous/>



References:

1. Fine-Grained Password Policy in Active Directory - http://woshub.com/fine-grained-password-policy-in-windows-server-2012-r2/
2. Introduction to Active Directory Administrative Center Enhancements (Level 100) - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-#bkmk\_create\_fgpp

~ End of Practical 2~