**Secure Microsoft Windows**

**Practical 5**

**Planning and Deploying Patch Management**

|  |
| --- |
| **Objectives:**  After completing this lab, you should be able to:   1. Understand the basic installation and configuration procedures of WSUS 2. Configure Group Policy for Windows Update 3. Approve / test specific updates for your domain workstations 4. Use WSUS Report Wizard to check for installed Updates |
|  |

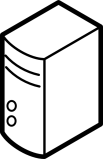
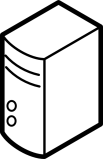
Lab Prerequisites:

In this Lab, you will need 3 virtual machines: A Primary Domain Controller, a Windows 2012 R2 (serve as a WSUS client), and a Win Server 2016 member Server with the WSUS role.

Your virtual machines need to have a reliable connection to the Internet in order to complete the lab.

As a domain administrator, instead of letting all the windows workstations / servers to download the latest Windows updates/patches from the Internet, you shall install a centralized software update server such as Windows Server Update Services (WSUS) on a member server and let it takes care the download of all the updates needed for your entire network. You need to configure the targeted windows machines in your domain to check for updates from the particular local WSUS server. In this practical exercise, we only set the windows server 2012 R2 to use the local WSUS services.





Windows Server 2012 R2 – gets updates from Server2

Server2 – WSUS Server installed and getting updates from Microsoft

Domain Controller

checks for update from the Internet.

**Lab Exercise 5-1: Preparing a standalone server with the Windows Server Updates Services (WSUS) role**

**(Warning! WSUS service requires more memory than any other servers in the smw lab. (try to adjust the memory allocation for all the involved VMs accordingly. Recommended minimum Memory – 3 GB. If possible, set 4 GB memory to your WSUS server)**

There are two options for you to choose from to setup your new member server WSUS role.

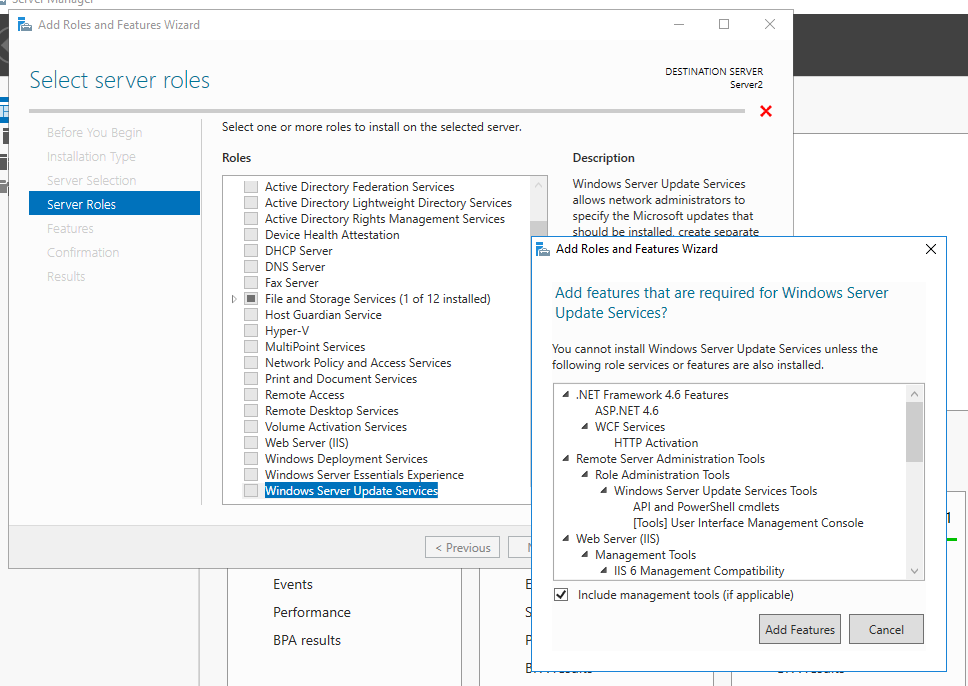
Option 1: (Recommended)

1. You may download a pre-built Image, Lab5\_wsusServer\_2023.zip, from the usual SMW OneDrive folder ([The Link](https://ichatspedu-my.sharepoint.com/:u:/g/personal/karl_kwan_ichat_sp_edu_sg/EWWK5QX37T5LmiecdnNlqvQB0MeXhgwf-_zHF59abMCbJA?e=bv73uj)).
2. Unzip the VM image from the zip file.
3. Power on the Domain Controller first. (The domain controller is a vital part of your domain, so it should always be on!)
4. Power on your new VM, configure and check that you have network access to the Domain Controller and have the Internet access. (ie. Use you PDC as the preferred DNS and set the correct gateway IP.)
   1. The default local admin user is ladmin, password is '1qwer$#@!'.
   2. Based on your experience form the previous exercises, accomplish the following basic configurations:
   3. The basic configuration includes: (but not limited to)
      1. Computer Name. (Change it to Server2 or other meaningful name of your choice.)
      2. Time Zone
5. You may check for and get the latest windows updates for this VM.
6. That’s all, you may proceed to EX-5-2 now.

Option 2: (For your consideration only – it may take 2 to 4 hours to complete the following process)

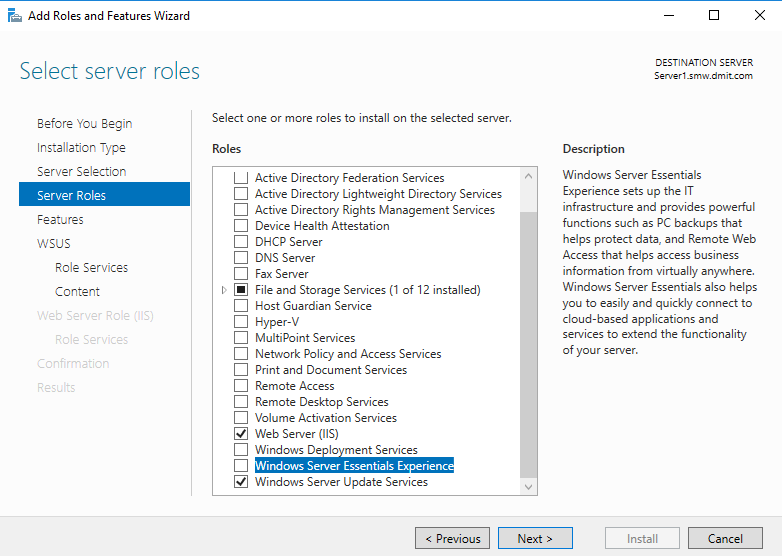
You will install the Windows Server Update Services (WSUS) on a new member server (Server 2016)

1. Power on the Domain Controller. (The domain controller is a vital part of your domain, so it should always be on!)
2. You can use the Windows Server 2016 baseline VM image (from Lab 1) and use it to configure it as your Server 2. (Just make sure you choose the ‘I copy it’ option when you start the image)
3. Power on your Baseline VM, configure and check that you have network access to the Domain Controller and have the Internet access. . (ie. Use you PDC as the preferred DNS and set the correct gateway IP.)
   * The default local admin user is smw\_srv2016, password is '1qwer$#@!'.
   * You may check for and get the latest windows updates for this VM before proceeding to the next step.
   * Based on your previous exercises, accomplish the following basic configurations:
   * The basic configuration includes: (but not limited to)
     1. Change your virtual machine name (at VM settings) to wsus\_server.
     2. Computer Name. (e.g. Server2)
     3. Rename the local admin user account from smw\_srv2016 to ladmin , or you may add in a new account and name it ladmin, this is to avoid confusions at the later part of the exercise.
     4. Time Zone
4. At this point, your new Server2 VM is tapping onto the DHCP and DNS services of your domain, but it is still running as a standalone server. Other than that, it does not have other relations with your domain.
5. Before proceeding to the next step, please ensure your Server2 is compliant to the following two requirement:
   * Your Server2 has good connection to the Internet.
   * Your Server2 should have ~15 to 20 Gb free disk storage at this point.
6. On Server2, login as Local Admin. Start Server Manager and try to add in a new Role – Windows Server Update Services

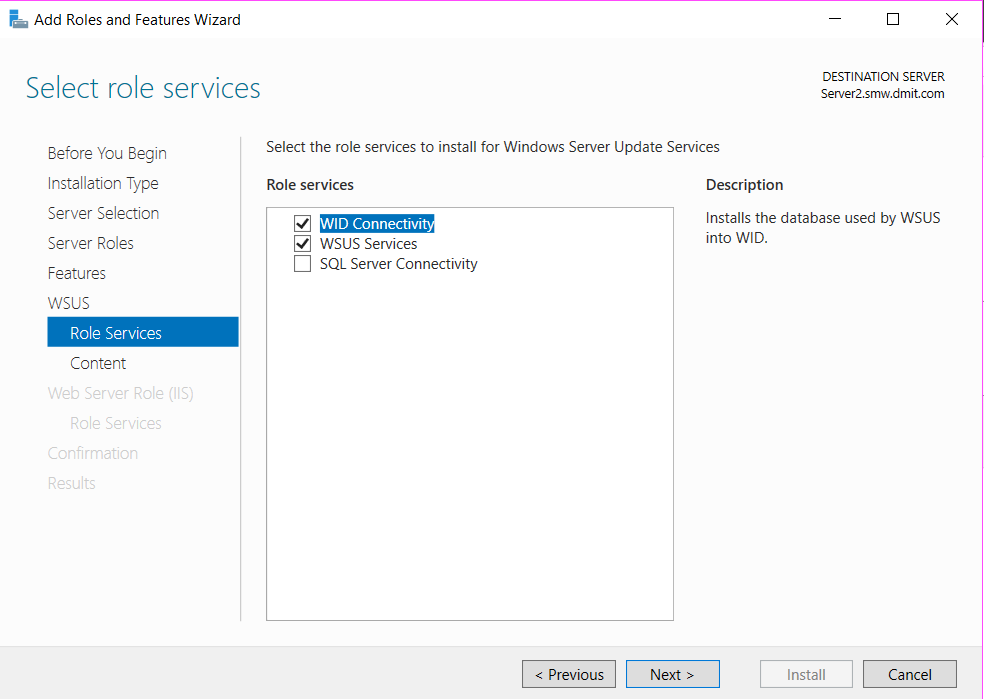


1. Take the default choices and press ‘Add Features’ at the Add Role and Features Wizard.

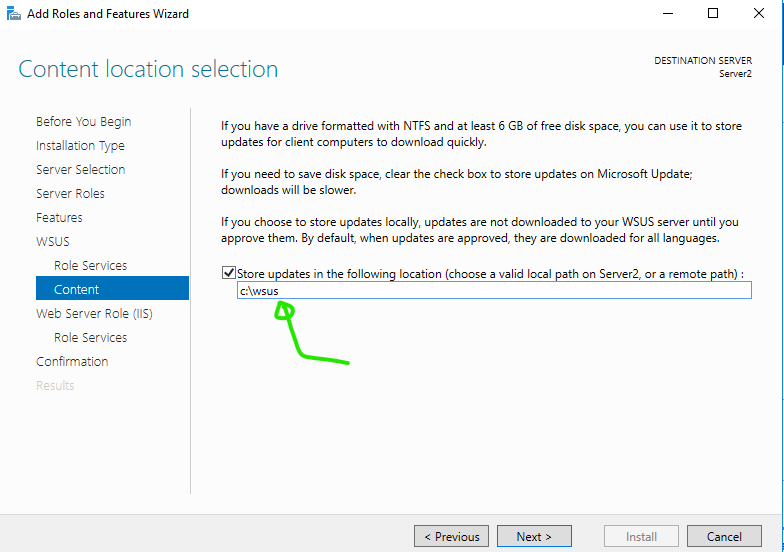
Take note of what are the required additional roles and features (including web server IIS) for adding in WSUS role.



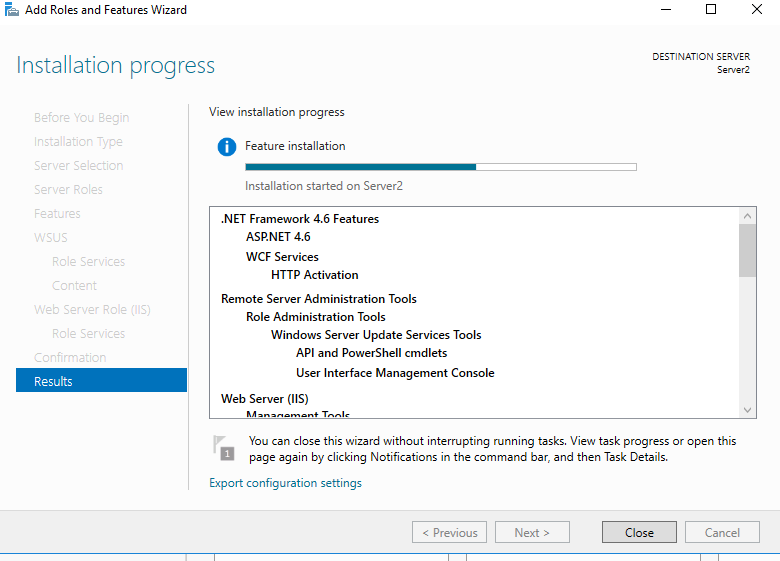
1. The Wizard will be refreshed the Select Server Roles screen and you may Click Next to accept and proceed to install all the required features. There will be a few more option screens, and you can accept all the default options/selection to proceed. One of them (showing at below) is worth to mention, as it gives you the choice of databases to store the windows updates content. In our case we pick the default option, as we do not have a MS SQL database in our domain. WID is a kind of standalone database that can be used to support the WSUS operations.



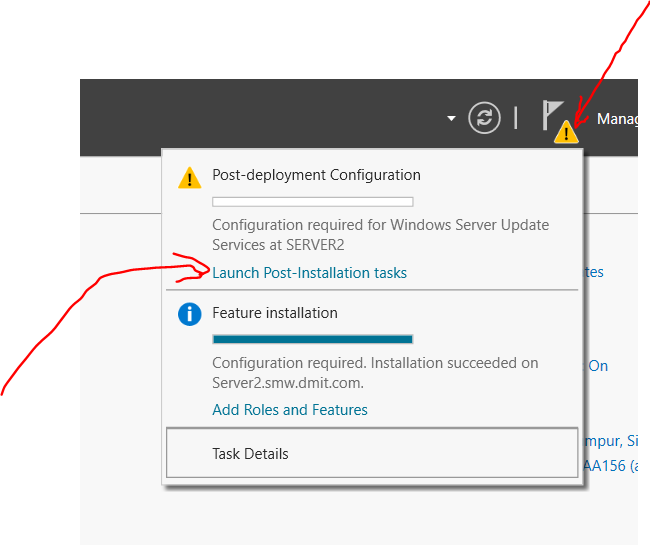
1. When the Content location selection appears (see following diagram). Read carefully of the descriptions and the different choices. You may choose to store the updates at the local path, ie. C:\WSUS. (\* The wizard will create this local folder automatically).



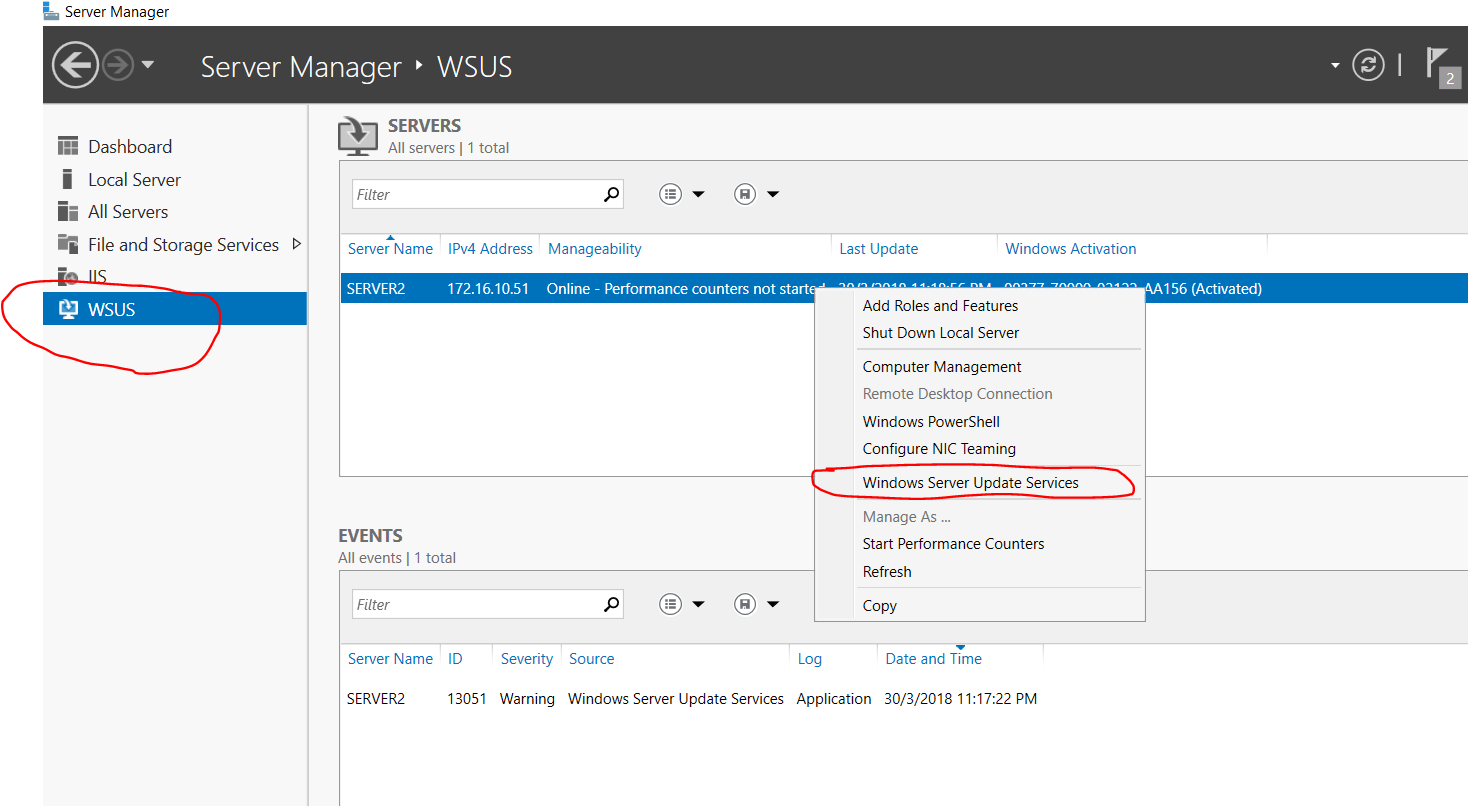
1. The wizard will then proceed to first install the dependent roles and features follow by installing the WSUS role. Be patient as this may take for a while.



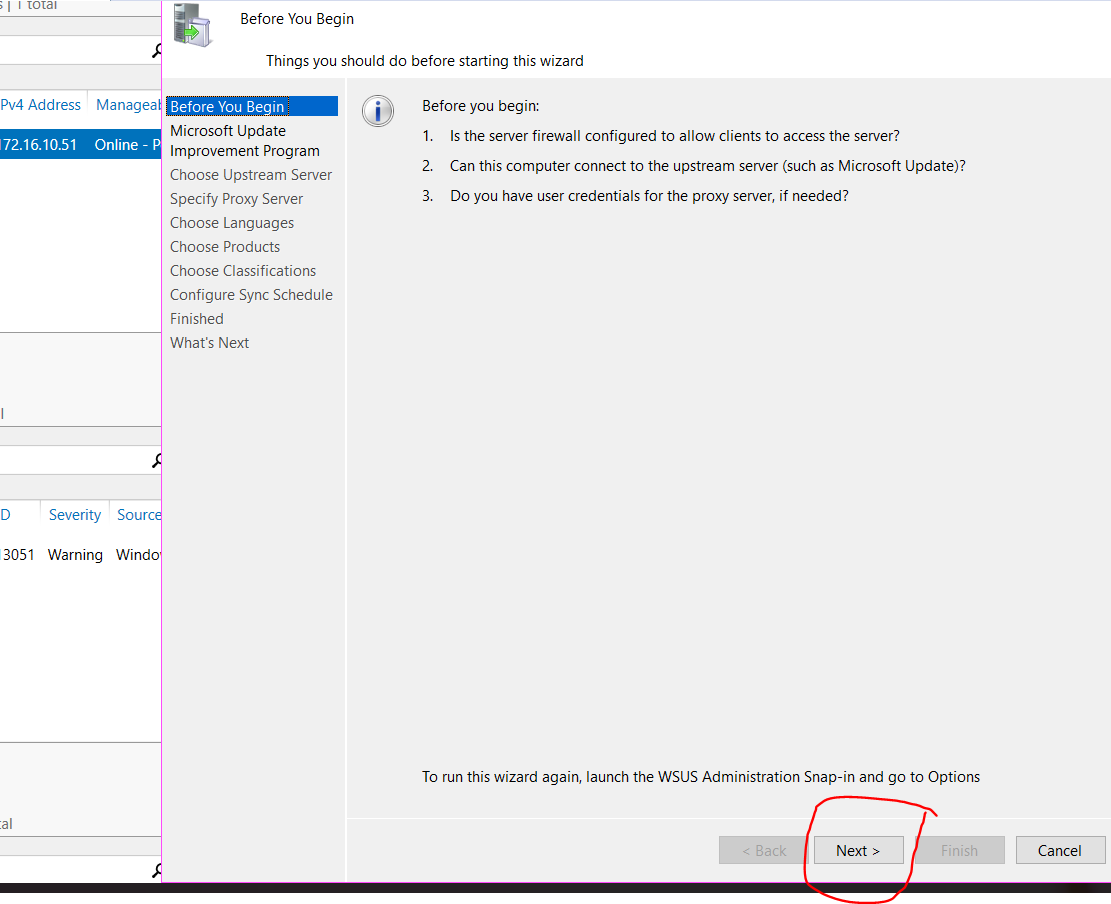
1. Once the installation is completed, the system will display an 'alert' notification that, post-deployment configuration is required. You may click on the ‘Launch Post-Installation tasks’ to proceed. In fact, this implies the installation process is getting into the next stage. Just wait for **a little while longer**, you will see the installation and configuration are proceeding accordingly.



1. Eventually, you will see the Windows Server Update Services appears at the left pane of the server manager. You can select the WSUS Node and right click on the main pane and execute the Windows Server Update Services management console.

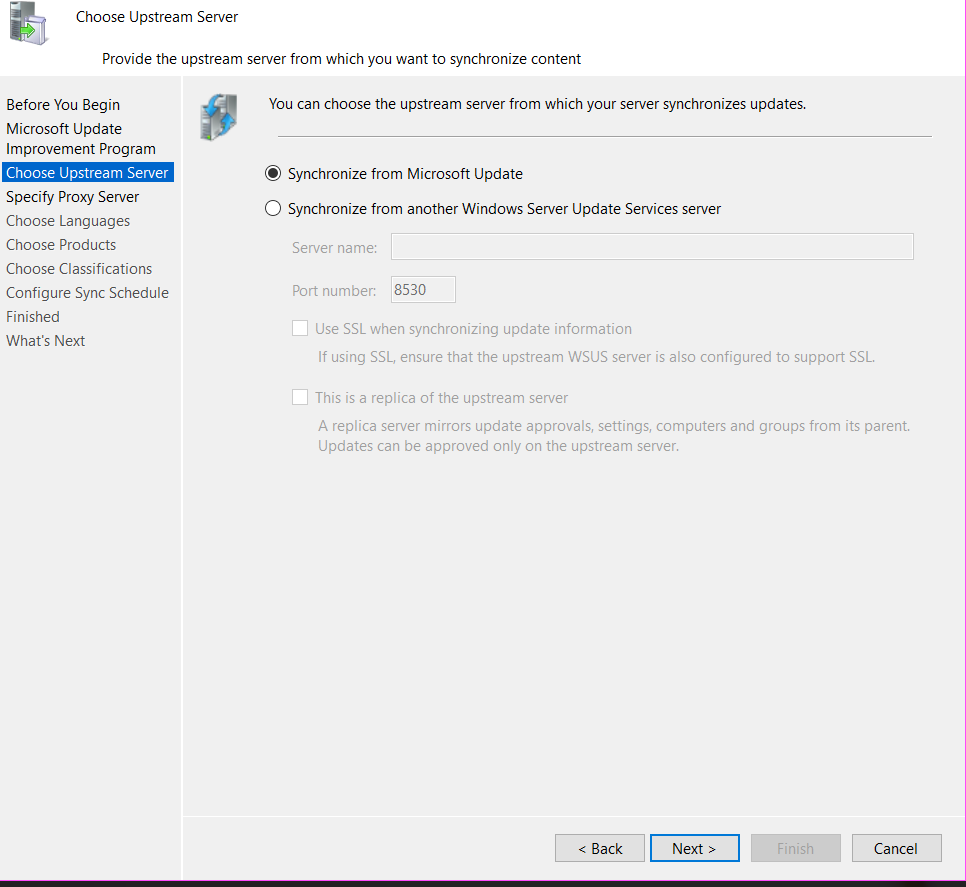


At the initial run of the WSUS management console, the Configuration Wizard will be popped up automatically, it will guide you through the configuration process.



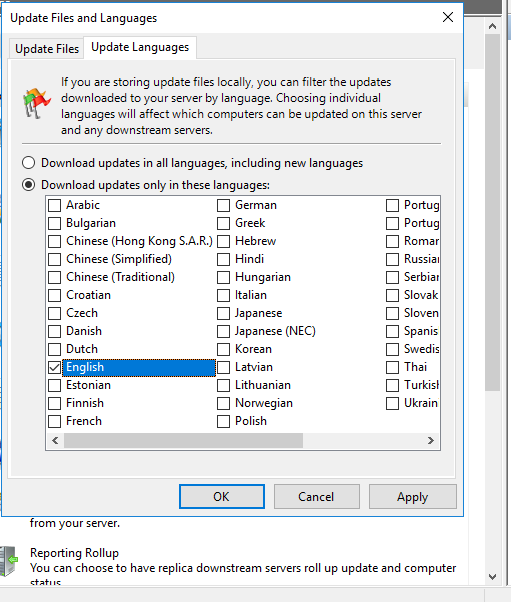
\*If you want to, you can run WSUS Server Configuration Wizard from the Options page of the WSUS 10.0 Administration console.

1. When asked to Choose Update Source (or Upstream Server), leave the default “Synchronize from Microsoft Update” checked. (See following diagram).

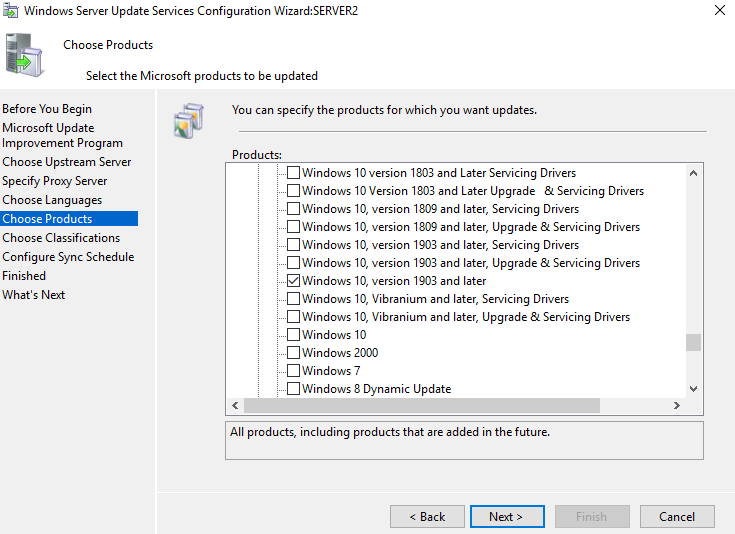
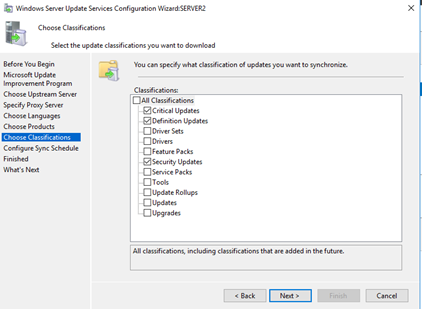


1. For Proxy Server, we do not need to specify a proxy in our lab to access Internet. Click OK to confirm your update source and proxy server settings at one go. Right after this, you will be prompted to proceed with the connection test (Initial synchronization), click ‘start connecting’ to proceed, and it will take a while until the wizard goes to the next step. [This initial Connection Operation may take up to an hour to complete.]

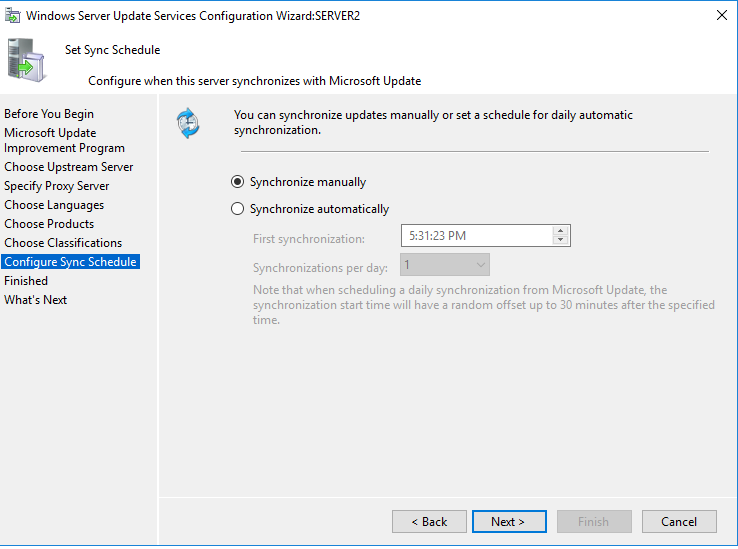
1. For Language choose the 'English' only to conserve storage requirement.



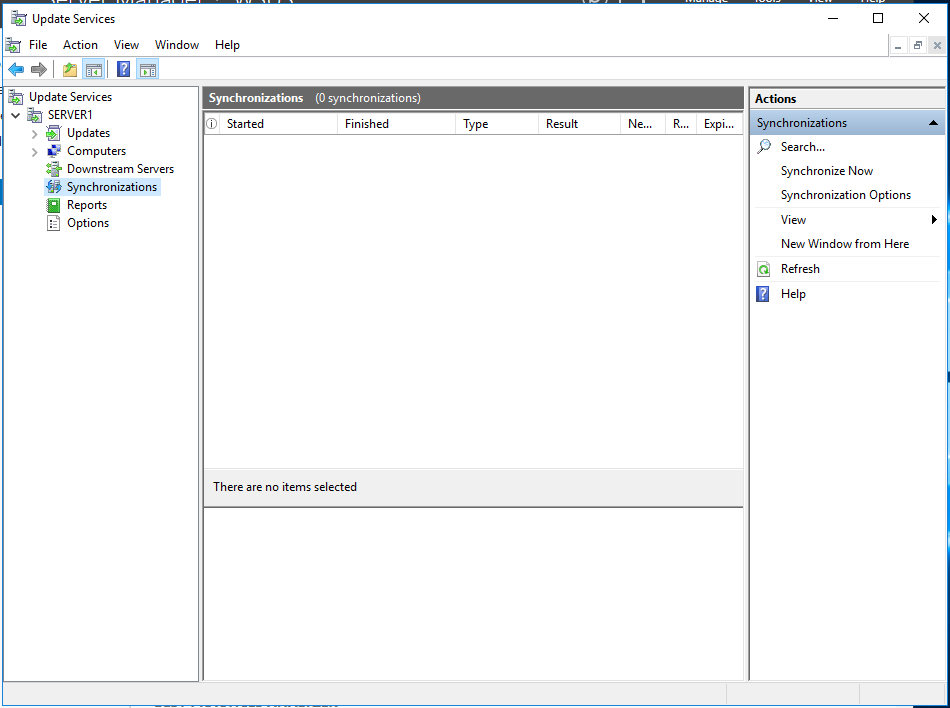
1. For Products and Classifications, try to make a sensible choice to only include minimum set of updates targeted for Windows Server 2012 R2 and take the default ‘classification’ choice. \*Special note! You may need to run at least once of the initial synchronization in order to obtain a complete Products and Classifications listings. The initial synchronization only take place when you are running the WSUS configuration wizard. In order to rerun the Wizard, you can find the command link as the last entry in the options pane (See step 12).



1. For Synchronization Schedule, take the default setting of 'manual', as we are not really trying to host a production WSUS which usually synchronizes with Microsoft Update in a regular basis.

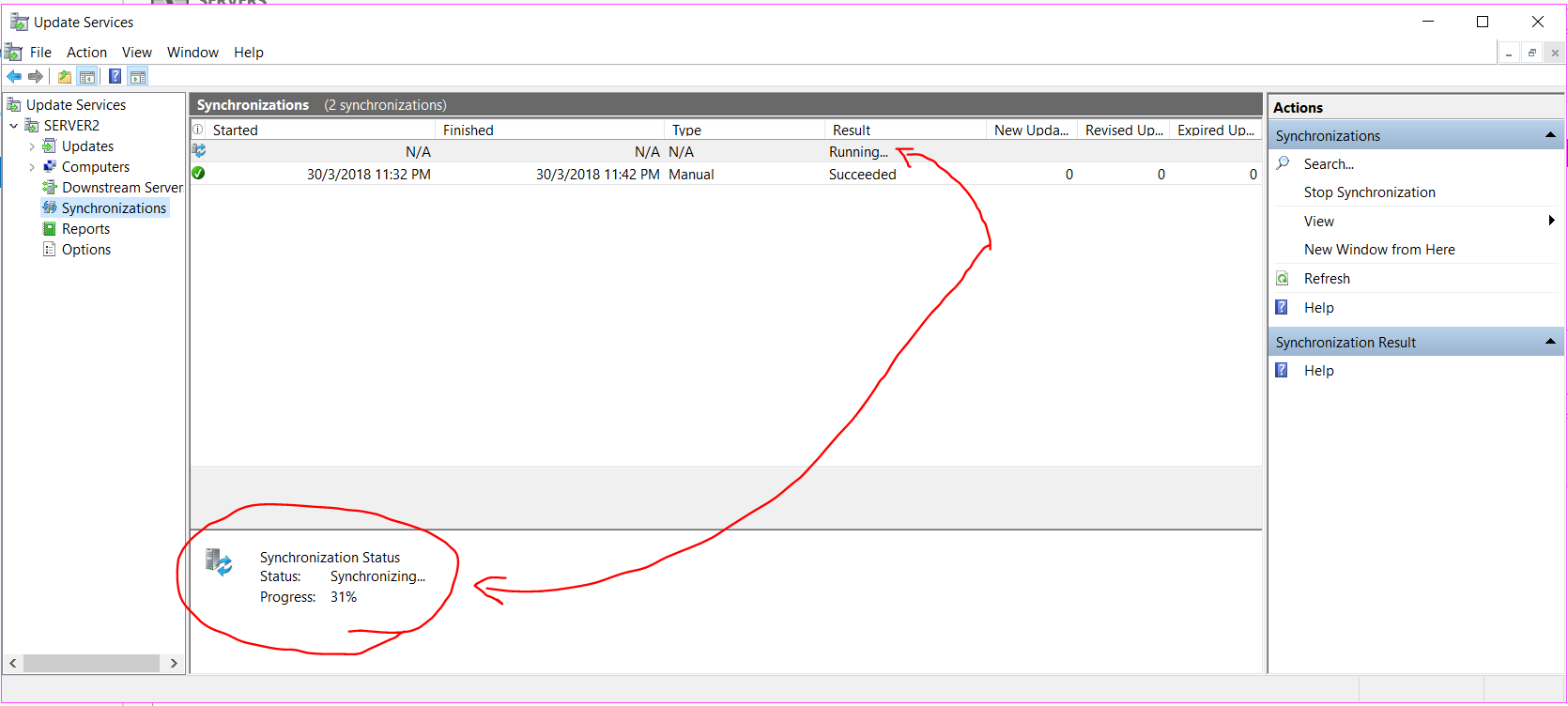


1. After all the basic configuration is completed, you may trigger the first Synchronizations operation (manually), by selecting the Synchronizations option from the left hand side menu, and click on the Synchronize Now under the Actions options at the far right :

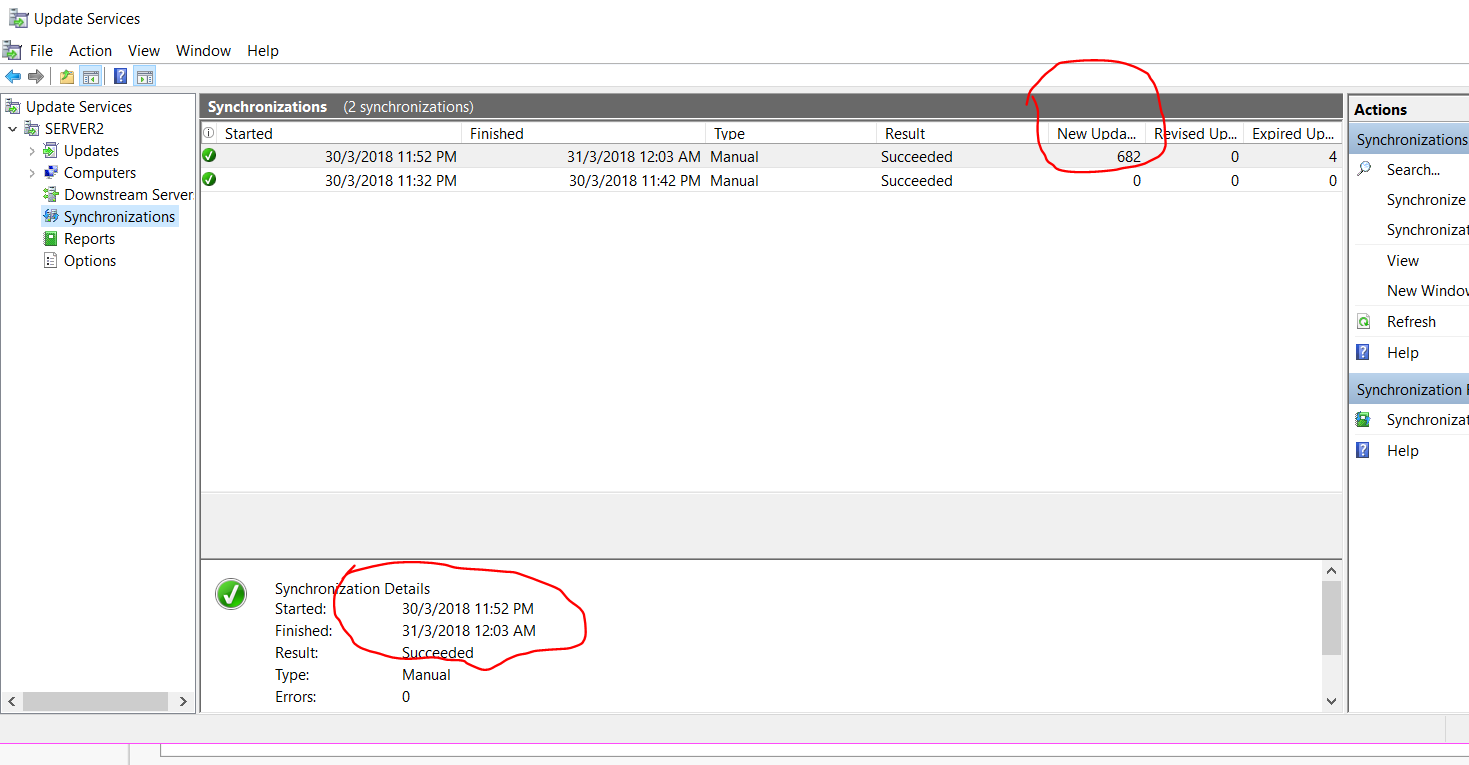


Depending on the choices of your products and classifications settings, this synchronization operation may **take a very long while (say >= 24 hours)**  to complete. Please consult your tutor before confirming your choice. In general, we recommend only include Windows Server 2012 R2 as product and definitions files update as the classifications.

1. The middle pane of the Synchronization menu will show the task that is currently running. (See the following diagram).



1. The synchronization is downloading updates for Windows 2012 R2. It may take about 5 to 10 minutes or longer depending on the connection speed and quality.



1. When the synchronization is complete, try to click on Synchronization Report in the right pane. You will get a message that you need Microsoft Report Viewer (2012 redistribution) in order to view reports.

As generally we do not use servers for browsing the Internet, we will use the Windows 10 image to search for and download Microsoft Report Viewer.

1. Using the Windows 10 image or simply your own notebook, open Internet Explorer and do a search for “Microsoft Report Viewer Redistributable 2012” or browse to <https://www.microsoft.com/en-sg/download/details.aspx?id=35747>
2. Download the Microsoft Report Viewer installation file.
3. Copy the downloaded msi file over to Server2 (you can use shared folders, or by other means, i.e. use drag and drop to copy the file from you notebook to the VM)
4. On Server2, close WSUS console if it is still running. Install Microsoft Report Viewer (2012 redistribution).
5. While you are installing the Microsoft Report Viewer, the installation wizard may prompt you to download some other Microsoft components. Just follow the given instruction and proceed.
6. In WSUS Console, click on Synchronizations in the left pane. In the middle pane, select the latest Synchronization that you just did. In the right pane, click on Synchronization Report to see the updates for Windows Server 2012 R2 that were downloaded. Below is a screen shoot of a sample report :

Graphical user interface, text, application

Description automatically generated

Congratulation to you, up to this point, you have successfully installed the WSUS service.

**Lab Exercise 5-2: Joining your WSUS Server to your domain.**

1. Before you have joined to the domain successfully, you should set and confirm that network Connection Settings of the WSUS Server accordingly.

* Static IP address
* Gateway
* DNS (Ensure the DNS is referring to your domain DNS)

1. Now you can let your standalone server to join to your domain.

Firstly, you must assign an appropriate static IP address to your standalone WSUS server.

Secondly, you can apply the same approach you have learnt from the previous labs to let this server to join to your own domain.

However, you may encounter some issue as it is not allowed to have machines with the same SID co-exist in an Active Directory.

Graphical user interface, text, application

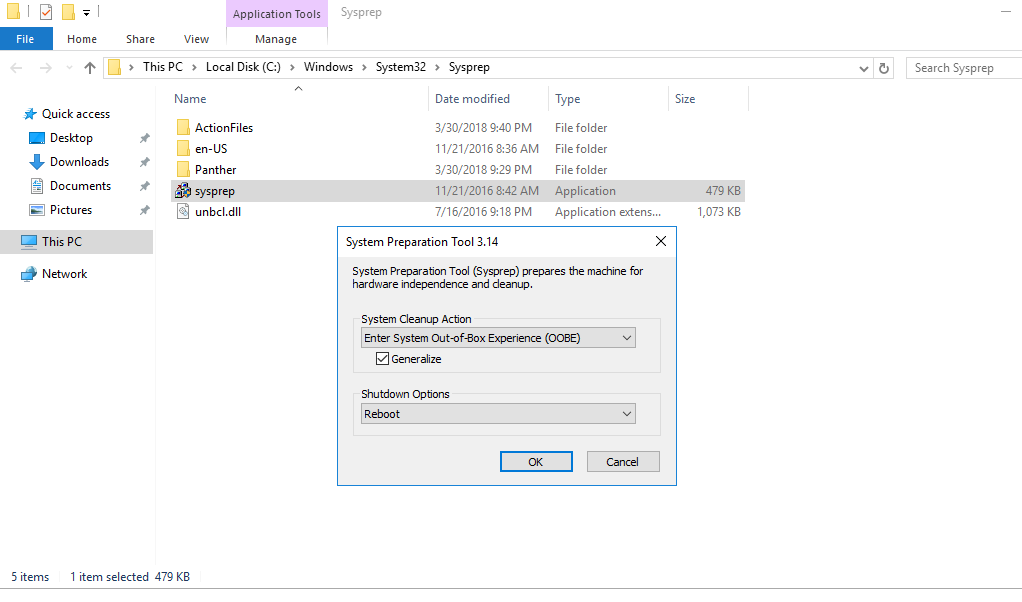
Description automatically generated

In case you have encountered an error message similar to the one as shown above: You need to regenerate a unique SID for the new server image:

At the standalone VM, right click on the Window button, open a Run Box and enter ‘sysprep’ and press enter.

The folder which contains the sysprep application will be opened.

Run the sysprep application using administrator privilege:



Choose the default option with a tick on the Generalize. (See the above), press OK to proceed.

Reflection prompt: While waiting for the operation to complete, you may go to search what this sysprep is for. [Here](https://techcommunity.microsoft.com/t5/windows-blog-archive/the-machine-sid-duplication-myth-and-why-sysprep-matters/ba-p/723859) may provide you some answers.

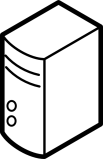
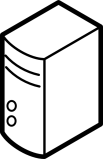
1. Once the system is rebooted and reset, you should notice that the computer name has been assigned with a random value. Set it back to ‘Server2’ (or your preferred value) before proceeding to the next step.
2. Before you try to join to the domain again, you should set and confirm that network Connection Settings of the WSUS Server accordingly.

* Static IP address
* Gateway
* DNS (Ensure the DNS is referring to your domain DNS)

Now, join your server to the domain.

**Lab Exercise 5-3: Setting up WSUS Client Configuration (STOP HERE)**

You will now create a Group Policy for your Windows Server 2012 R2 (Server 1 you have setup since lab 3). The Group Policy will make your Windows Server 2012 R2 VM checking for updates from the WSUS service running on Server2 instead of from the default Windows Update services at the Cloud.



Check for updates

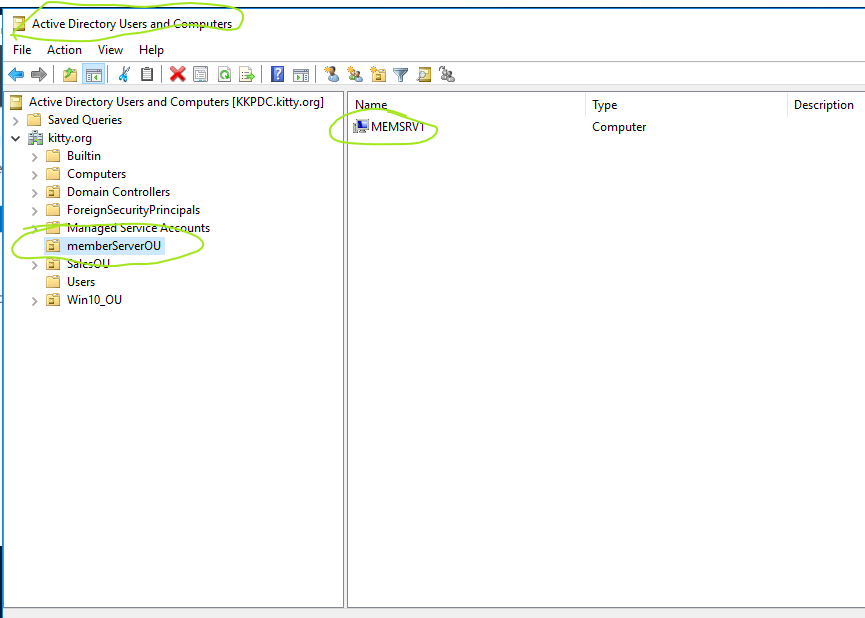
Domain Controller: Let Windows Server 2012 R2 receive a group policy object which configures the client to check for updates from the WSUS Server

WSUS Server (Server2)

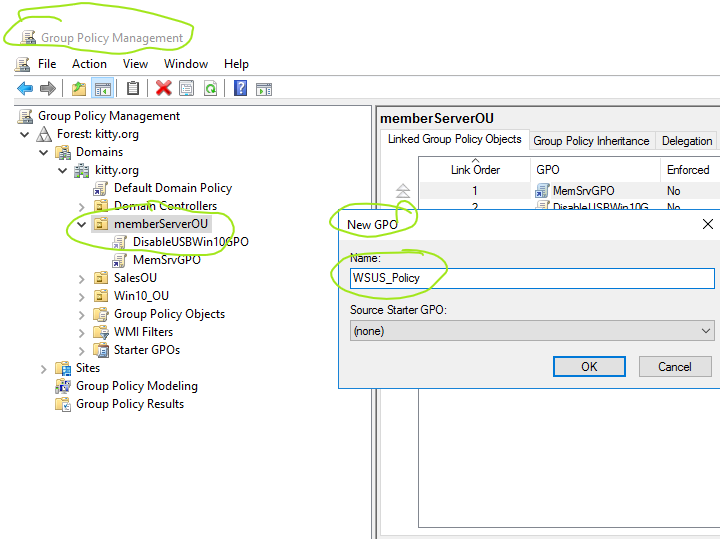
Windows 2012 R2

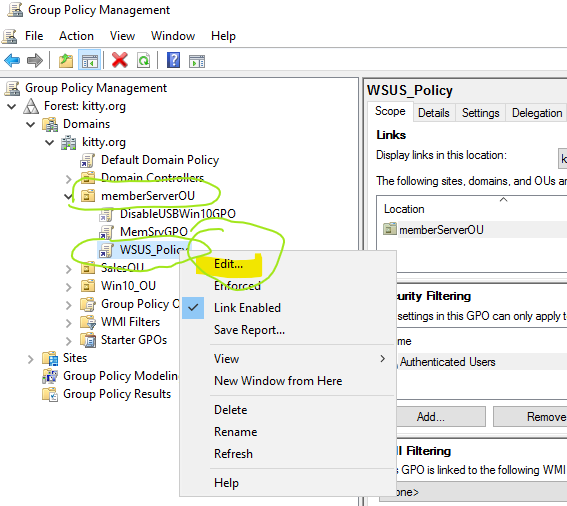
(Server1)

1. On the Domain Controller, use Active Directory Users and Computers, verify if there is an OU called "memberServerOU". Create one if it is needed. Move your Windows Server 2012 R2 (Server1 or other name you have assigned it to be.) to this "memberServerOU".



1. Run Group Policy Management Console (GPMC). Right-click on the memberServerOU in the left hand pane and choose Create a GPO...
2. For Name, enter “WSUS\_Policy”. Click OK.



1. Expand the memberServerOU. Right-click on WSUS\_Policy and choose Edit.
2. 
3. Make the following changes to the policy:

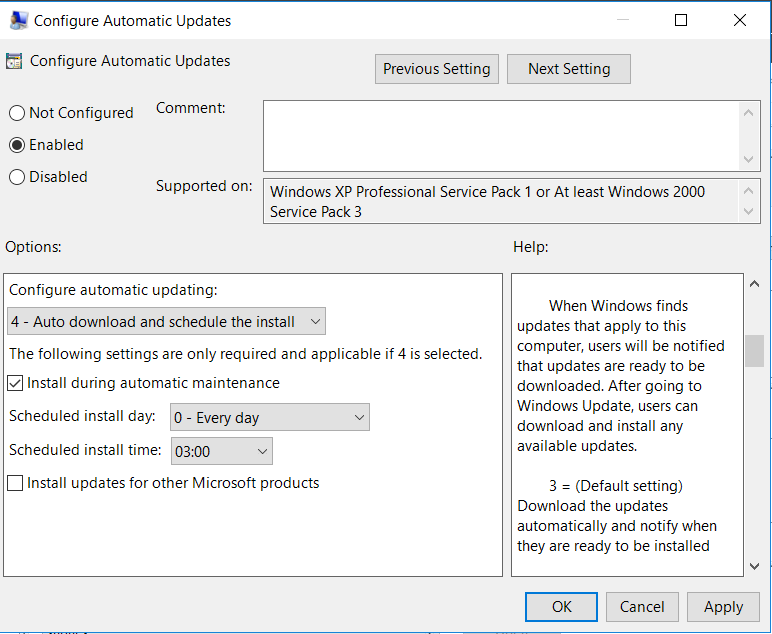
Computer Configuration-> Policies -> Administrative Templates -> Windows Components -> Windows Update

1. Double-click “Configure Automatic Updates”.

Click Enabled. Select “4 - Auto download and schedule the install”. (See the following diagram)

Or you can select option 3 (The default). For the later choice you will see the update effect much faster in the following Ex 5-5.

Tick the Check box of Install during automatic maintenance



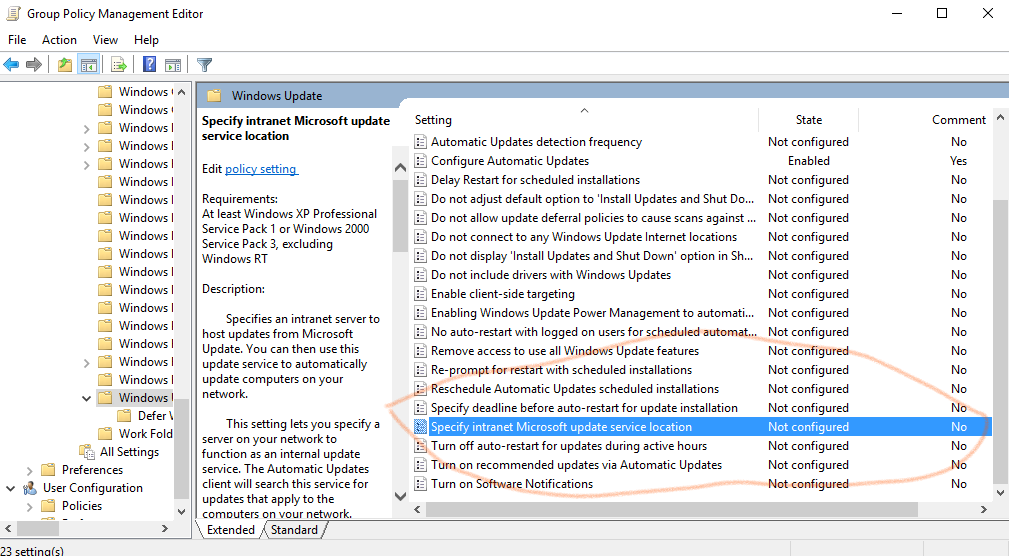
1. Click OK.

Reflection Prompt: Study the difference between the Option 2 to Option 5 setting.

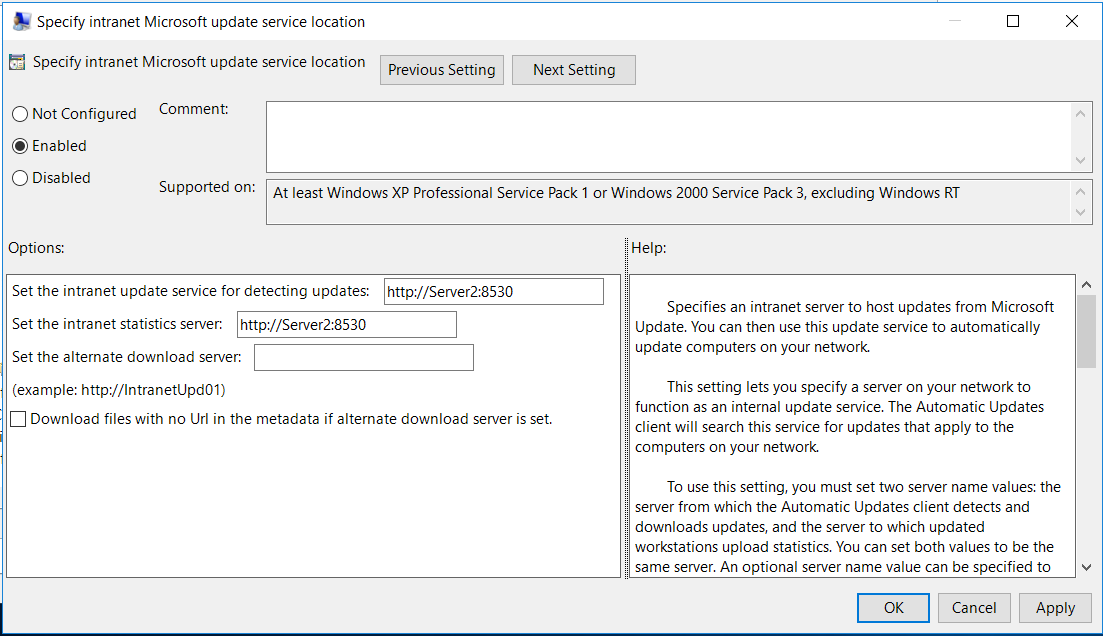
Option 2: Notify for download and install

Option 5: Local admin can choose a setting

1. Double-click “Specify Intranet Microsoft Update Service Location”.



1. Click Enabled. Type “http://Server2:8530” for both the “intranet update service for detecting updates” and the “intranet statistics server” (you can also replace “Server2” with the IP address of Server2) (see following diagram). Take note that, the http service port of the WSUS (later than 6.2) has been changed to 8530.



1. Click OK.
2. You may also check out the “Automatic Updates detection frequency” setting. (Optional)
3. Close the Group Policy Management Editor.

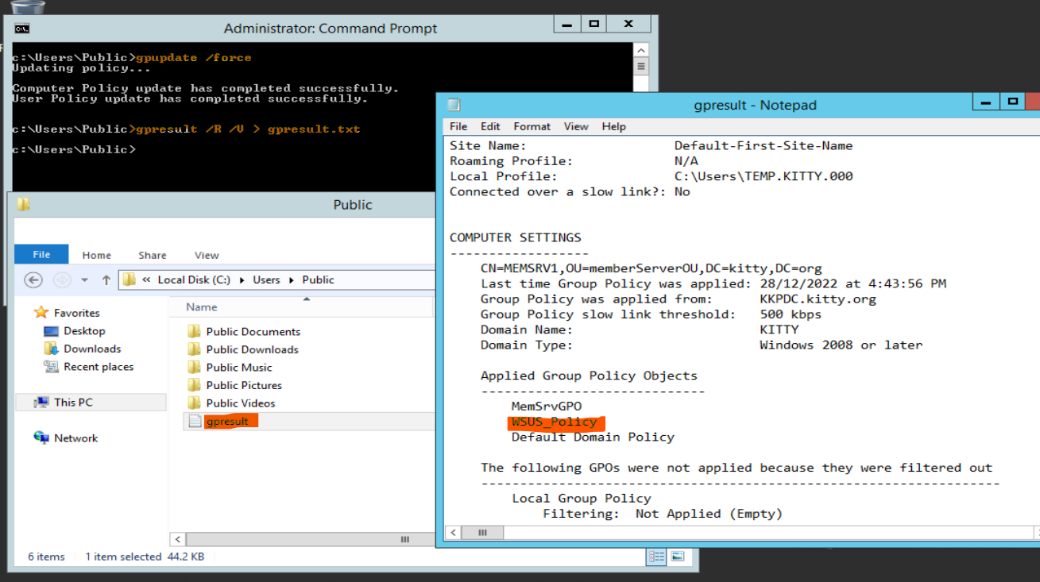
To get the Group Policy applied to your Windows 2012 R2 immediately:

1. Power on your Windows Server 2012 R2 (if needed).
2. On the Windows Server 2012 R2 as domain administrator, at command prompt or power shell (run as Administrator) , run “gpupdate /force”.
3. To verify if the update WSUS settings have been applied to your Win server 2012 R2 via the GPO, you can use the gpresult command :

GPRESULT /R /V

* To display the actual GPO setting, you need to run the command with Administrative Privilege.
* You may also need to ‘pipe’ the out to a text file, as the output is fairly long
  + cd c:/Users/Public
  + gpupdate /force
  + gpresult /R /V > gpresult.txt

Here is sample session of the getting a gpresult.txt by gpresult /r /v command:



After the Group Policy has been applied to the Windows Server 2012 R2, it may take about 20 min for the Windows Server 2021 R2 to contact the WSUS Server.

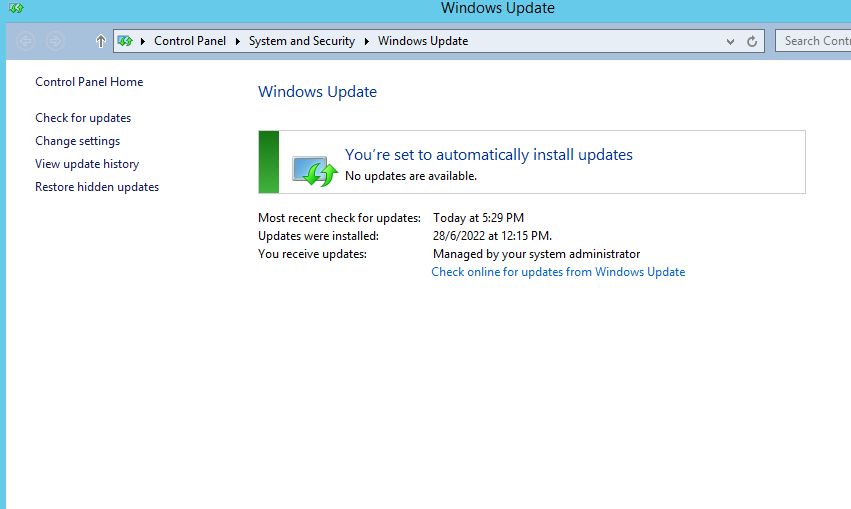
1. Check for updates interactively/explicitly.
   1. At the local server dash board of the server manager
   2. Click on the link next to the Windows Update
   3. Click on the Check for updates button at the popup.

Graphical user interface, text, application

Description automatically generated

Note: For newer windows: e.g., To force a Windows 10 Client to contact the WSUS Server immediately, run the Windows Update Auto-Update Client by typing "usoclient.exe startscan".

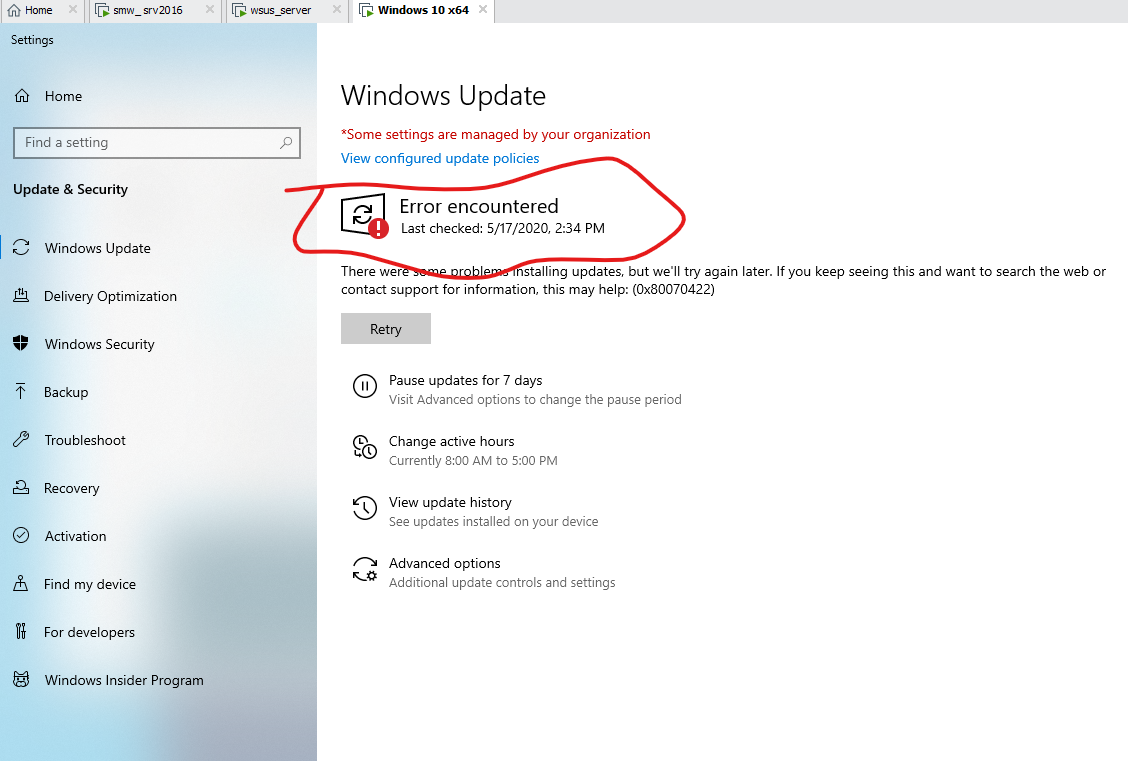
1. What you should be getting will be similar to the following:



As the server1's update process is controlled by the WSUS server now. There is no approved update for server1 to use at this initial moment.

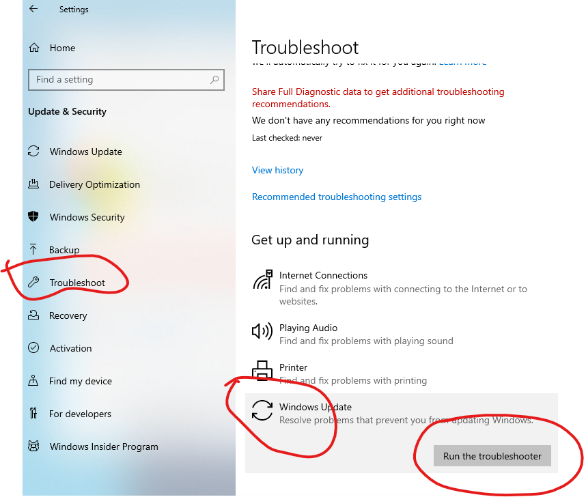
1. Trouble shooting common Windows Updates issue on windows 10 or later: **(Optional)**

In case you have encountered Error message after applying the “Check for Updates”:

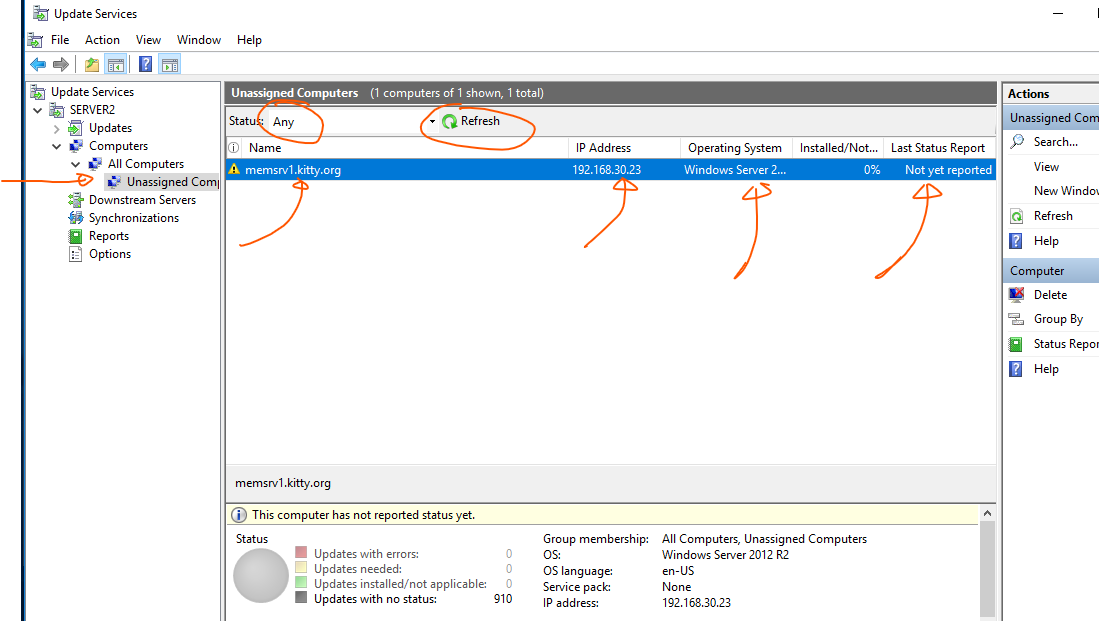


You may try resolve the problem by using the updates troubleshooter

At the Setting >> Update and Security , click on the troubleshoot at the left pane. At the main pane, click on the Windows Update and press the “Run the troubleshooter” button.



1. Check that the Windows Server 2012 R2 appears in WSUS on Server2:
   1. On Server2, login as Domain admin, run WSUS management console.
   2. In the left hand pane, expand Computers, All Computers, Unassigned Computers.
   3. Change the Status to “Any” and click Refresh. (see following diagram)\*



Your server 2012 R2 computer name should appear

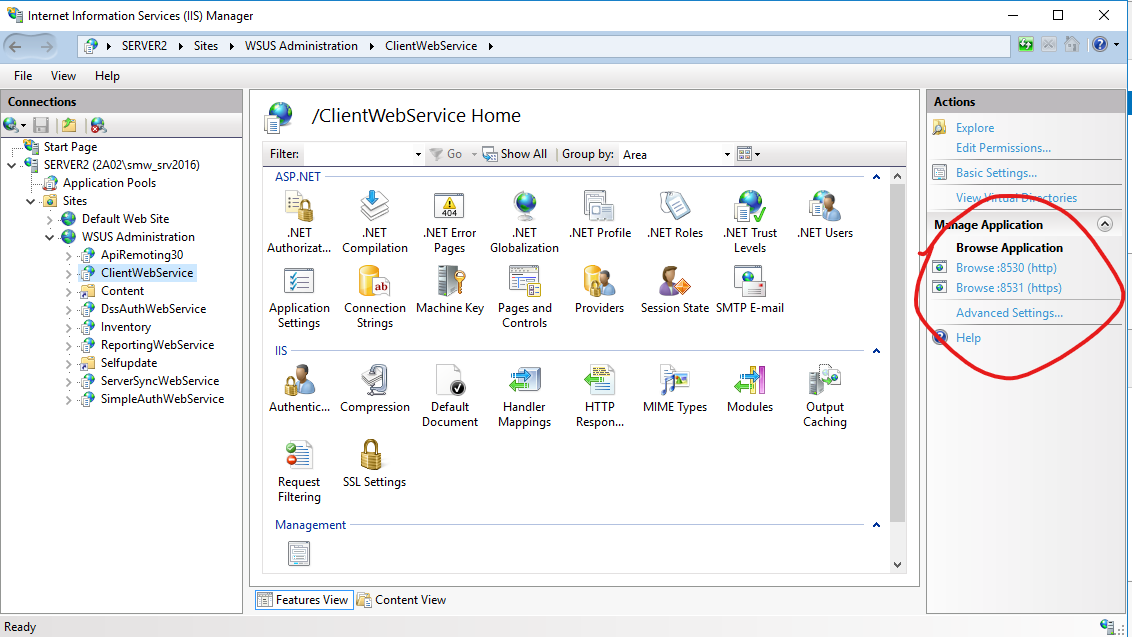
As you can see from the above, the client machine has not reported its status to the WSUS server yet.

\*In case you cannot see any computer listed, you may right click on the "Computer" label and choose 'search' option to force the Active Directory Search to load in the computer information.

**Lab Exercise 5-3-1: Verifying the downstream and upstream WSUS service ports (Optional)**

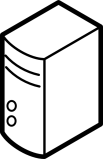
You may explore the usage of IIS Manager and verify which ports are being used for the WSUS service:

e.g.



**Lab Exercise 5-4: Set up a Test Computer Group to test updates from WSUS**

We can create a computer group with test computers that receive the updates first. If the updates do not cause any problems on the test computers, then the updates can be approved for the rest of the computers.

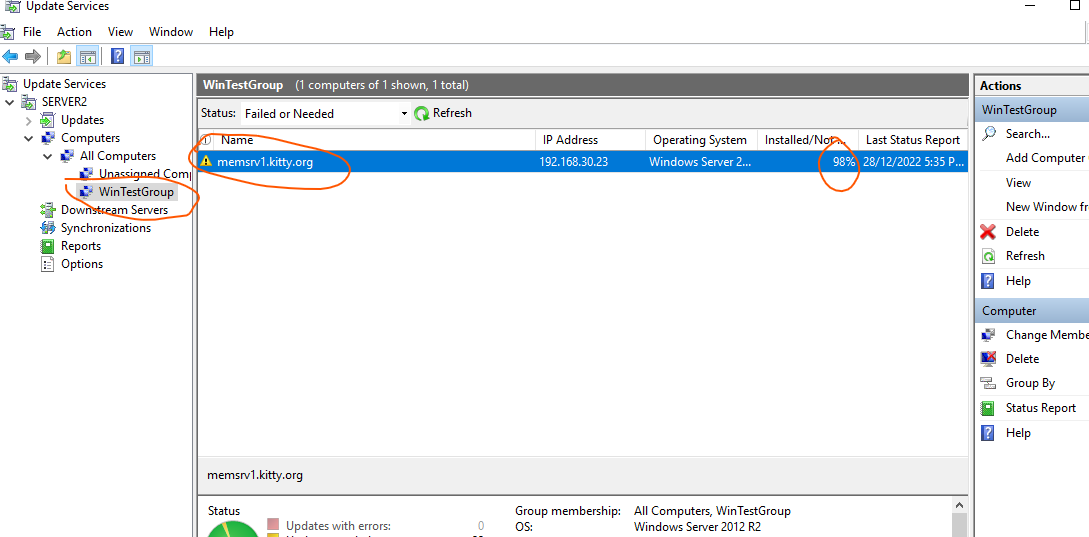


Updates approved for the Test Group first for testing.

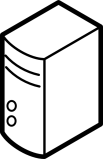
WSUS Server (Server2)

Test Group

1. On Server2, at WSUS management console, in the left hand pane, expand Computers, Right-click on All Computers and choose Add Computer Group.
2. For Name, type “WinTestGroup”. Click Add.
3. In WSUS, in the left hand pane, click on Unassigned Computers. Right-click on your Windows 2012 R2 client and choose Change Membership.
4. Select WinTestGroup and click OK.



**Lab Exercise 5-5: Approve and Deploy updates to the Test Group**

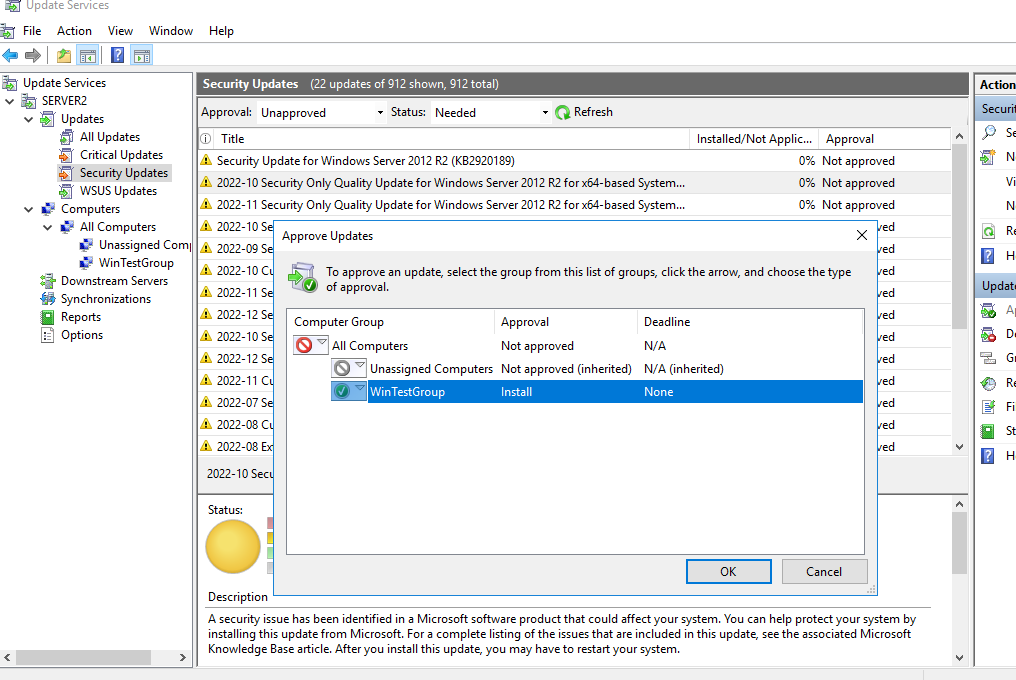


Approved update downloaded to Test Group

Test Group

WSUS Server (Server2)

1. On Server2, in WSUS management console, in the left hand pane, expand Updates. Click on Security Updates.
2. For Approval, choose Unapproved. For Status, choose Needed. Click Refresh. (see following diagram)
3. Select any one or two of the updates and Right-click on it/them and choose Approve. (see following diagram)

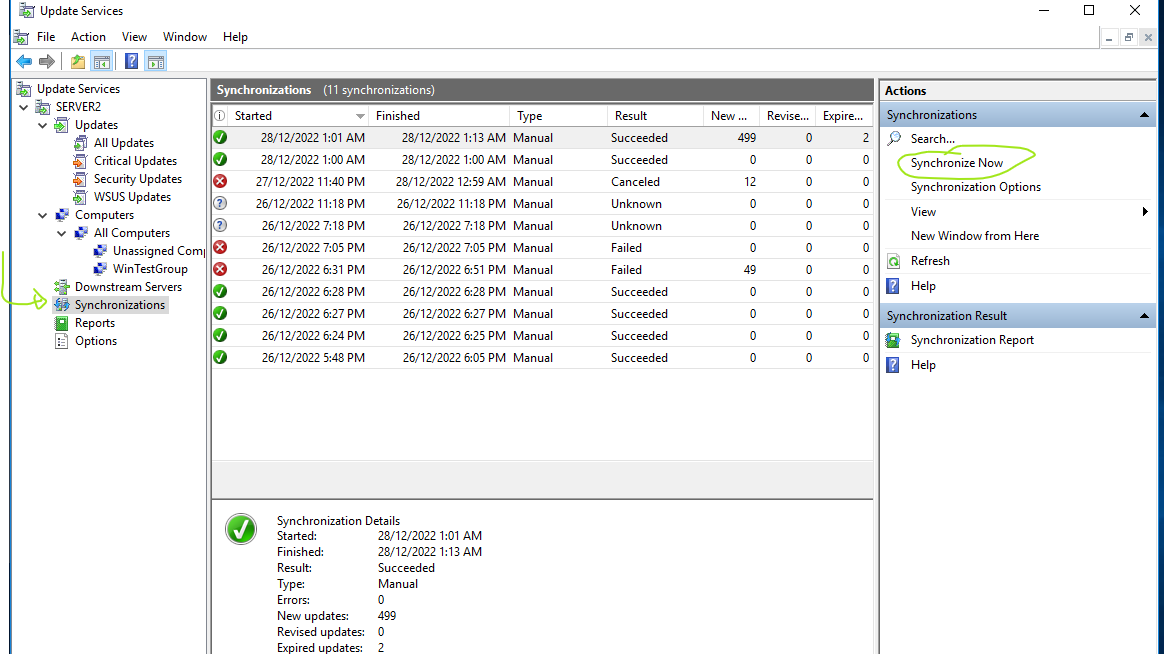


1. Click OK.
2. Change the Approval dropdown to Approved. Click Refresh. You will see the approved update listed. (see following diagram)

Graphical user interface, application, Word

Description automatically generated

1. The update you have approved will be downloaded from Microsoft at the next synchronization process.
2. Do a manual synchronization Now (See the following diagram):

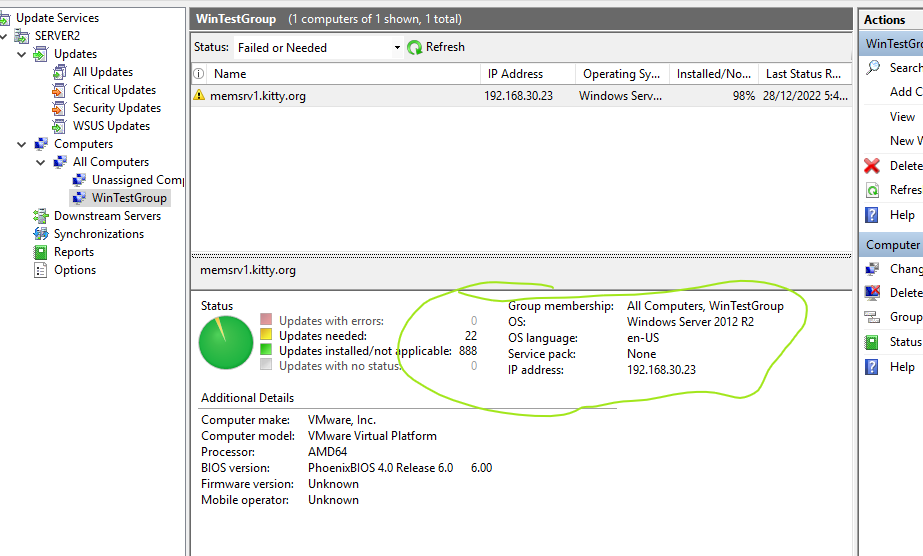


1. By default, clients will check the WSUS for updates every 22 hours. To make the Windows Client check for updates immediately, you need to do it manually.

1. **Eventually**, at your Windows 2012 R2, you will see the update will be automatically downloaded and pending for installation without the user intervention.
2. Install the update. Restart the Windows Server 2012 R2 if necessary.

You will now look at the Windows Update Status Report for your Windows Server 2012 R2:

1. On Server2, in WSUS console, expand Computers, All Computers. Click on WinTestGroup. Right-click on your Windows server and choose Status Report. You should be able to observe that the report is now different from the one you have seen at Exercise 5-4 step 4. You can browse through the pages of the report to see the updates that have been installed for the Windows Server 2012 R2.



~ End of Practical 5 ~