Lab 15:

Windows Server   
Update Service

Windows Server Security  
 2024-2025

© Daan Pareit

## Introduction

# Lab concept

In this lab we’ll install and configure Windows Server Update Service (WSUS).

# Learning goals

* Installing WSUS on a Windows Server Core
* WSUS initial configuration
* WSUS update management
* WSUS GPO settings

# Practicalities and prerequisites

You’ll need to run the following VMs (as configured in the previous labs):

* Your Windows Server Core (KING) and Windows 11 client (DESKTOP-XXXXXXX) VM.
* Your pfSense VM for Internet access

## WSUS installation

**General remark:** In this lab, we’ll install the WSUS server feature on our Domain Controller (DC) Server. Because the DC has a very important role in the network, Microsoft typically advises limiting the number of additional features that are installed on the DC. In this way, the DC’s attack surface (security risk) and chance of crashes (availability risk) are minimized. For large-scale production networks, you should therefore consider using a separate non-DC server for WSUS (potentially combined with other roles and features). The reason we’re installing WSUS on the DC server in this lab is to minimize the number of VMs (and thus disk space and memory usage) on your system.

We will deploy the WSUS role on KING.

* Create a C:\WSUS folder on KING. We will use this folder later to store the WSUS updates.

A screenshot of a computer

Description automatically generated

* On KING, execute the following command to get a list of currently installed roles and features:   
  Get-WindowsFeature | where installed -eq true

A screenshot of a computer program

Description automatically generated

* Now, use the RSAT Server Manager (from the Windows 11 VM or your own laptop) to remotely add the ‘Windows Server Update Service’ role to the KING server.
* You can accept the default proposed settings for additional features and role services (WID and WSUS services).
* For the storage location, specify the “C:\WSUS” folder on KING, which you recently created.
* The wizard will propose to add yet another Role. Which role is this? Accept the proposed additional settings.

It additionally asks to install IIS (Windows Web Server)

* In Server Manager, click the ‘flag’ icon for notifications. Click the ‘launch post-installation task’. Give it a few seconds and it will automatically finish the post-installation tasks behind the scenes.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Logon to KING, and list again the installed roles/features. Compare this to the earlier list.

A screenshot of a computer program

Description automatically generated

This is the most important thing that got changed (quite a lot of packages installed)

* Now, back at the Windows 11 VM, note the new WSUS category in your Server Manager (left sidepanel). However, have a look at the available tools in Server Manager (top right menu). We don’t have a WSUS tool yet.
* Therefore, on the Windows 11 VM (and/or on your laptop), install the Windows Optional Feature: “RSAT: Windows Server Update Services tools”.

OH NO A WINDOWS FEATURE AGAIN!!!

Installed

## WSUS initial configuration

We will configure the WSUS update distribution on KING.

* Start the WSUS tool from the Server Manager (on the Windows 11 VM or on your laptop).
* In the tool, connect to king.company-XXXX.serverlabs.be or 192.168.11.50 . (Note: if you run the tool from your laptop, you’ll have to choose ‘manage as’ and provide Administrator or domain admin credentials and start the WSUS tool from within Server Manager, else you’ll get a confusing error message about the post-installation task and SSL.)

A screenshot of a computer

Description automatically generated

* You will be presented with an initial configuration wizard. If you aren’t or if you exited the wizard too early, you could launch it again from the WSUS tool in the ‘Options’ section by choosing “WSUS Server Configuration Wizard”.
* Accept the default settings and start syncing with Microsoft Update to get the information about the available updates. This step can take a while (>15 minutes)! (On Howest campus, you can choose to sync with our WSUS upstream server instead: 172.20.4.43 . This will be faster.) What is the default port used for syncing between WSUS servers (without SSL)?

8530 seems to be the default port

A screenshot of a computer

Description automatically generated

I had an error on this so had to reboot both of my machines.

* Continue the wizard. To minimize the number of updates here, only select the following:  
  (Note: if you have chosen the Howest upstream WSUS server, you won’t have any choice.)
  + Language: English
  + Products: ‘Windows 11’, ‘Windows 11 Dynamic Update’ and ‘Windows 11 GDR-DU’

A screenshot of a computer

Description automatically generated

* + Classifications: Definition Updates / Critical Updates / Upgrades

A screenshot of a computer

Description automatically generated

* + - Note: thus, disable the ‘Security Updates’. Again, something you don’t do in production environment, but here this is done for the sake of minimal VM disk space, waiting time and network load within the lab while we can still configure all WSUS settings.
* Choose manual synchronization, check ‘Begin initial synchronization’ and finish the wizard.
* In the ‘Update Services’ tool, have a look at the ‘synchronizations’. There you’ll see the sync progress and how many updates you synchronized afterwards.

A screenshot of a computer

Description automatically generated

## WSUS update management

* Now, at the ‘updates’ category you can see the different available updates. Note: you’ll need to change ‘status’ to ‘any’

A screenshot of a computer program

Description automatically generated

* In the WSUS tool, you can define computer groups which need the same type of Windows updates. Define a new WSUS group ‘desktops’ (via right clicking on ‘all computers’ at the ‘computers’ section).

A screenshot of a computer

Description automatically generated

* If you go back to ‘updates’ and select a random update and click ‘Approve…’ you will now see that you can (dis)approve this update for ‘desktops’ group specifically. What are the different options?

A screenshot of a computer

Description automatically generated

Approved for Install

Approved for Removal

Not Approved

We now want to have all our regular domain computers (not the servers) to be part of this ‘desktops’ WSUS group to update according to the update settings of this WSUS group. These computers are part of the OU ‘PCs’, of which e.g. DESKTOP-XXXXXXX is a member (cfr an earlier lesson). (If you didn’t, you can quickly create this OU via the ADU&C tool of the Server Manager and drag and drop DESKTOP-XXXXXXX into it.) We thus need to link this OU with the ‘desktops’ WSUS group

* First, we need to set in the WSUS settings that computer assignments to groups will be done via GPOs. Therefore, find in the ‘Options’ in the WSUS tool where to change how computers are assigned to WSUS groups. What is the name of the item in the ‘options’ section where you specify to use GPOs for computer assignments into WSUS groups?

Options > Computers > Use Group Policy or registry settings on computers

A screenshot of a computer

Description automatically generated

* We also need to configure this in our domain policy. At your Windows 11 VM, open the Group Policy Management Editor and create a new GPO linked to the ‘PCs’ OU.

A screenshot of a computer

Description automatically generated

* In this GPO, we’ll have to change some settings for “Windows Update”. Go to Computer Configuration – Policies - Administrative Templates – Windows Components – Windows Update – Manage Updates offered from Windows Server Update Service
* Now, we ‘ll change the “Specify intranet Microsoft Update service location” policy to indicate that KING should be used as the WSUS server for the computers of the OU ‘PCs’ .
  + Remember the additional role which had to be installed when installing the WSUS role? The Windows updates are sent over the web; thus this is a URL of KING. Note that you can indeed browse to http://king . What web page is shown?

A screenshot of a computer

Description automatically generated

Default IIS web page.

* + WSUS is, however, not available at port 80 but at another port. Which one was that again? (You can find this in the WSUS options for the ‘update source’). Set the url with appropriate port in this “Specify intranet Microsoft Update service location” policy by using “http://king:<port>” as value. (And set the same value for the statistics server field.)

The port is 8530.

A screenshot of a computer

Description automatically generated

I hope it should look like this?

A screenshot of a computer

Description automatically generated

* Next, we want to indicate that all computers in the OU ‘PCs’ need to be linked to the ‘desktops’ WSUS group. Do this via the “Enable client-side targeting” policy. What value do you need to set here?

A screenshot of a computer

Description automatically generated

Target group name: desktops.

A screenshot of a computer

Description automatically generated

* Logout and login on the Windows 11 VM, perform a ‘gpupdate /force’ (force a group policy update). Verify then whether DESKTOP-XXXXXXX is indeed automatically added to the ‘desktops’ group in the WSUS tool (set the ‘status’ dropbox to ‘any’ to see DESKTOP- XXXXXXX).   
  (Note: You might need to have ‘Windows Update’ check for updates once on DESKTOP-XXXXXXX and then refresh the list in the WSUS tool.)

Had issues with the computer to appear in the list. A screenshot of a computer

Description automatically generated

To solve this, added the same rules to the other GPO that we had from previous lab (useless to do this)

Deleted and created the group in WSUS again (useless to do this)

Went and clicked to check for updates in the Windows settings and it worked.