WSUS – Setup Connected and Disconnected Servers

This guide provides the general steps needed to setup two WSUS servers: one that connects to the internet and Microsoft, and one that is disconnected from the internet on some internal network.

See the notes at the end of this document for additional observations and tips I’ve come across managing the WSUS server.

# Connected Online WSUS Server Setup Steps

Refer to TechNet: <https://technet.microsoft.com/en-us/library/hh852344(v=ws.11).aspx>

1. **Install** Windows 2012 R2
2. **Turn off the Firewall in the control panel and stop/disable the firewall service**
3. **Rename** the server to the hostname it needs to be
4. **Shutdown** server
5. Go into VM settings and **add another HDD**. This will hold the WSUS content.
6. **Power on** server
7. Go into **Disc Management**, **initialize disc**, and give it drive label of **E:\** and call it “wsus\_files”
8. Create a **new folder** in E:\ called “wsus”
9. **Restart** the server
10. Run a **Check for Updates** to update the server itself.
    1. You might get the error that ends in …19 (I think that’s the one), but it means you need to keep trying to connect for updates. It should work after the 3rd or 4th try.
11. **Restart** the server
12. Check again for any remaining necessary updates. Restart if needed.
13. Install WSUS Role (refer to <https://technet.microsoft.com/en-us/library/hh852344(v=ws.11).aspx>
14. Enter “e:\wsus” (assuming E:\ is the partition you created earlier) as the **Content Location Selection**
15. Proceed to “Step 3: Configure WSUS” in the TechNet guide
16. Only choose EN-US for language
17. For **Choose Products** only select the bare minimum required.
    1. Example: For my proof-of-concept build, I’m only choosing Microsoft > Windows > Windows 7
18. For **Choose Classifications** only choose bare minimum required. I chose Critical Updates, Security Updates, Update Rollups.
19. Finish configuring – but DO NOT tell it to do initial sync
20. Edit the Automatic Approvals to auto approve Critical and Security updates for the types of systems. In my case, only Windows 7
21. Once that’s done, Start Synchronization. This will take some time.
22. Once synchronization is successfully complete, go to the WSUS dashboard to view the progress of update downloads. All approved updates will need to be downloaded from Microsoft to the WSUS server. This will take some time.
    1. Example: After first synch, which showed 1,304 New Updates and 61 Expired Updates. The dashboard shows “Updates needing files: 1,035” a total of 10,937.39 MB.
23. **Copy** the WsusContent folder to be transferred to the disconnected WSUS server.
24. **Export** the metadata to be imported into the disconnected WSUS server.

# Disconnected WSUS Server Setup Steps

Refer to TechNet: <https://technet.microsoft.com/en-us/library/cc708513(v=ws.10).aspx>

1. **Install** Windows Server 2012.
2. **Rename** the server to the hostname it needs to be
3. **Shutdown** the server
4. Go into **VM settings** and **add another HDD**. This will hold the WSUS content. Consider the hard drive space required for the number of products and services that the server will be patching. 300 GB is a safe start size.
5. **Power on** server
6. Go into **Disc Management**, **initialize disc**, and give it drive label of **E:\** and call it “wsus\_files”
7. Create a **new folder** in E:\ called “wsus”
8. **Restart** the server
9. **Turn off the Firewall in the control panel and stop/disable the firewall service**
10. **Restart** server
11. **Install** WSUS Role (refer to <https://technet.microsoft.com/en-us/library/hh852344(v=ws.11).aspx>
12. Enter “e:\wsus” (assuming E:\ is the partition you created earlier) as the **Content Location Selection**
13. **Launch Post Installation tasks**
14. **Restart** the server
15. Proceed to “Step 3: Configure WSUS” in the TechNet guide to understand what you’re about to set.
16. In Server Manager go to **Tools** > **Windows Server Update Service**
17. The WSUS config wizard will start. Close it. It’s useless to run on the disconnected import server. You will set the settings manually next
18. Open the WSUS module, and go to **Options** > **Products and Classifications**
19. **Copy** over WsusContent folder from the connected WSUS server to the disconnected server
20. **Import** metadata to disconnected server
21. **Approve** the updates you need. Typically this will be every update that was imported, so you can Select All, Right-Click, and Approve for Install.
22. You may need to wait a few hours for WSUS to “download” update files. Basically it’s re-synching all of the metadata for newly approved updates with the actual update files you copied over in WsusContent. You can watch the progress from the WSUS dashboard under the “Download Status” section. You will see **Updates needing files** and **Downloaded** **xxxx.xx MB of xxxx.xx MB** that show the progress.

# Update Cycle Process

1. Log in to the internet-connected WSUS server
2. Open the **WSUS Management Console**, go to **Synchronizations** and choose **Start Synchronization**
3. Once Synchronization finishes, go to WSUS Dashboard and monitor the status of the **Updates Needing Files** section. This will show the progress of WSUS downloading the new content files for the patches it just synchronized from Microsoft. Keep WSUS online and connected until it pulls down all the files it needs, and the section shows **Updates Needing Files: 0**.
4. Go back to **Synchronizations** and choose **Start Synchronization**, to make sure that WSUS has pulled every new patch down from Microsoft. Repeat steps 3-4 until Synchronizations show 0 new patches synchronized.
5. **Connect an external HDD** to the internet-connected WSUS server, and **copy** the contents of the E:\wsus\wsuscontent directory to the external HDD. If you have last month’s copy of the WsusContent directory on the external HDD, you can use the ROBOCOPY command to do a differential copy, which will only copy over those files that are new. This will save you a lot of time. Here is the syntax of the ROBOCOPY command to use:
   1. **robocopy <source> <destination> /e /r:3 /w:5**
   2. example: robocopy e:\wsus\wsuscontent x:\wsusexports\wsuscontent /e /r:3 /w:5
6. Next, **export the metadata**. Open an **administrative command prompt** and navigate to the **C:\Program Files\Update Services\Tools** directory. Run the following command (this can take over an hour if there are a lot of updates in WSUS):
   1. **Wsusutil.exe export exportfile.xml.gz exportfile.log**
   2. Example: wsusutil.exe export export041917.xml.gz export041917.log
7. **Copy** the metadata export.xml.gz file over to the external HDD.
8. Properly eject/disconnect the external HDD from the internet-connected WSUS server
9. Connect the external HDD to the disconnected WSUS server
10. Copy the WsusContent directory from the external HDD over to the disconnected WSUS server using ROBOCOPY:
    1. **Robocopy f:\wsusexports\wsuscontent e:\wsus\wsuscontent /e /r:3 /w:5**
11. Copy the metadata export.xml.gz file over to the **C:\Program Files\Update Services\Tools** directory on the disconnected WSUS server
12. Import the metadata export.xml.gz file into the disconnected WSUS server. Open an administrative command prompt, navigate to the **C:\Program Files\Update Services\Tools** directory, and run the following command:
    1. **Wsusutil.exe import <exported file from prev server> <import log filename>**
    2. Example: wsusutil.exe import export041917.xml.gz import041917.log
13. Open **WSUS Management Console**, and approve the new updates that were just added.
14. Go to the WSUS Dashboard overview, and monitor the progress of the **Updates Needing Files** section. WSUS will take some time to process and validate the new files. This is how the disconnected WSUS “downloads” the content files for those new patches.

## N O T E S

1. **Problem with WSUS server not pulling down all the updates it needs for itself.** After pointing the offline WSUS server to itself to pull updates (versus the default setting of it trying to pull from Microsoft’s servers) the server pulls down a chunk of updates, but not all of them. A fresh Windows Server 2012 R2 system will need around 150 updates installed to start. The disconnected WSUS server only pulled around 60, if I remember correctly. After that, the server would not recognize that it needed any more updates, and would display the “Your computer is up to date” message. However, ACAS showed that the server was missing a lot of updates still.

The fix I found, was that the server was missing a core update package that was almost like a Service Pack. Without that update, it couldn’t recognize that it needed additional updates because those additional updates technically didn’t apply – yet.

First install KB2919442 – this is a prerequisite for installing the major update package. Next, find KB2919355 package on the Microsoft Update Catalog. It contains multiple updates. You must install them in this order: clearcompressionflag.exe (an executable that does something under-the-hood and won’t display anything graphically), KB2919355, KB2932046, KB2959977, KB2937592, KB2938439, KB2934018. After that and many reboots after most of those KBs are installed, the WSUS server should be able to check for updates and recognize that it needs to pull down additional updates.