10.1. What is a WSUS?

Windows Server Update Services (WSUS) is a client-server application that allows you to use a server on your intranet as a centralized point for updating software. Without WSUS, clients must communicate with the Microsoft Update Web site to download and install patches and other updates. WSUS offers the following advantages:

- Clients receive updates from local servers rather than using Internet links to receive updates.
- You can control which updates clients in your organization receive.
- You can enforce the application of updates throughout your organization.

WSUS uses the following components:

Component	Description
Microsoft Update	Microsoft Update is the Microsoft Web site that provides updates for Microsoft products. Without WSUS, clients communicate directly with the Microsoft Update Web site to download updates.
Windows Server Update Services (WSUS) server	A WSUS server is a server that you configure within your private network and that you use to manage updates within your organization. • At least one WSUS server in your organization communicates with the Microsoft Update Web site to get a list of available updates. • On the WSUS server, you approve the updates that you want to install to clients in your network. • You can configure the WSUS server to download approved updates. Clients in your organization download updates from your WSUS server instead of the Microsoft Update Web site.

Automatic Updates	The Automatic Updates client is a component of client and server operating systems that downloads and installs updates on the local system. • By default, the Automatic Updates client communicates with the Microsoft Update Web site for updates. • When using WSUS, you configure the Automatic Updates client to get updates from your WSUS server. You can configure clients to download approved updates from Microsoft, or download updates from your WSUS server.

WSUS servers can be deployed as follows:

Deployment Scenario	Description
Single WSUS server	With a single WSUS server deployment: • You configure a single WSUS server on your private network. • The WSUS server communicates with Microsoft Update. Updates are approved on the WSUS server. • All clients are pointed to the WSUS server for update information. Use a single WSUS server for a small network at a single location.
Multiple independent servers	Using multiple independent WSUS servers is the same as using a single-server configuration, but with separate server groups. • Multiple WSUS servers are configured on the private network. For example, you might have a server in each site, or a server for each operating system used on your network.

	• Each server communicates with Microsoft Update. Updates are approved on each WSUS server. • Clients in each location or group are configured to use their corresponding WSUS server. Use this approach for large networks in different physical locations or for different groups when each server is managed separately.

Multiple synchronized servers	You can configure multiple WSUS servers in a parent-child relationship, and then synchronize approval lists and/or updates between servers.
	
	• One WSUS server is configured as the parent server and communicates with Microsoft Update. Child (downstream) WSUS servers are configured to point to the parent WSUS server.
	• The relationship of the child to the parent can be configured as follows:
	  o In autonomous mode, the parent server distributes updates, but approval is managed separately on the child servers.
	  o In replica mode, both updates and approvals are synchronized to child servers.
	• Client computers are configured to use the closest child server for updates.
	
	Use this approach for large networks with multiple sites. Choose autonomous mode for centralized administration, and replica mode for decentralized administration.
	
	Though there is no designated limit to the number of levels you can implement in a WSUS server hierarchy, Microsoft recommends that you implement no more than three levels due to the added lag time for propagating updates that occurs with each additional level.

Disconnected WSUS server	If you have a network that is not connected to the Internet, use the following method to implement WSUS: • Connect one WSUS server to the Internet and configure it to communicate with Microsoft Update. Configure updates and approvals on this server. • Export the settings from this WSUS server to removable media. • Configure a WSUS server on the disconnected network. Import the settings from the first WSUS server.

Microsoft Update and WSUS support updating the following products:

- Windows operating systems (2000/XP/Vista/7/10/2003/2008/2012/2016)
- Exchange Server 2000/2003/2007/2010/2013/2016
- SQL Server (all versions)
- Office (all versions)
- Microsoft ISA Server 2004/2006
- Microsoft Data Protection Manager
- Microsoft ForeFront
- Windows Live
- Windows Defender
- …and many other products (See full list on website of Microsoft Corporation)

You can control updates based on the following criteria:

- Product family (such as operating system version or product)
- Update classification (such as critical updates or drivers)
- Language

10.2. WSUS Server Configuration

Use the WSUS Administration Console to manage the server. You can use the console to manage remote servers that are running WSUS. Use the **\Update Services\Tools\wsusutil.exe** utility to manage WSUS from the command prompt.

The following table lists considerations for configuring WSUS on the server:

Task	Description

Installation	Install WSUS as a Server Role.
	• Windows Server 2008 requires WSUS version 3.0 SP1 or later. Installing WSUS requires IIS 6.0 and the .NET framework 2.0.
	• Windows Server 2012/2016 requires WSUS version 6.0 or later. Installing WSUS requires IIS 6.0 and the .NET framework 4.5
	• During installation, choose **Store updates locally** to download updates to the WSUS server.
	  o Updates are only downloaded after they are approved.
	  o You must have at least 6 GB of space on an NTFS volume to store updates.
	  o If you deselect this option, updates must be downloaded from the Microsoft Update servers.
	• You can store data about available updates in the Windows Internal Database, or to a SQL server database.

Configure the server	After installing WSUS, run the wizard to configure initial server settings, including: • Which server to use to synchronize with (either Microsoft Update or an upstream WSUS server) • Proxy server settings

	• Filter settings to filter by language, product type, and classification (critical updates, security updates, drivers, etc.) • The synchronization schedule At the end of the wizard, the server connects to the upstream server and synchronizes a list of possible updates based on the filter criteria you specified. The actual updates themselves are not downloaded until after you approve the update. After the wizard is finished, you can edit the settings in the **Options** area to modify the same settings configured during the wizard.

Approve updates	Only approved updates will be applied to WSUS clients.
	
	• You must synchronize updates before you can approve them. Synchronization downloads the list of updates based on your filter criteria.
	• After you approve the update, the update is downloaded if you chose to store updates locally.
	• Select the Options node to configure automatic approval settings:
	  o Approval rules identify criteria that is used to automatically approve updates.
	  o A default rule approves all critical and security updates.
	  o You can modify the default rule or create your own rules.
	  o Additional settings let you automatically approve updates to WSUS or to approve updates to previously-approved updates.

Add downstream servers	To add a downstream server, use one of the following options: • Install WSUS and run the wizard to configure the server as a downstream server. • Under the Options node, edit the Update Source and Proxy Server settings. Select **Synchronize from another Windows Server Update Services server** to make the server a downstream server to another WSUS server. Select **This server is a replica of the upstream server** to copy the approval and update list from the upstream server. After configuration, be sure to synchronize the downstream server with the upstream server, either manually or on a schedule.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

10.3. WSUS Client Configuration

Each client computer must have the Automatic Updates client software to use automatic updates. This software is included automatically with Windows Server 2016/2012/2008, Windows 10/7/Vista, Windows Server 2003, Windows XP Service Pack 1, and Windows 2000 Service Pack 4. It can be added to other operating systems as a special download. By default, clients contact the Microsoft Web site for updates. For a custom solution, configure clients to contact your WSUS server.

The easiest way to configure client settings is to use Group Policy to distribute the server name and other update parameters. The following table lists some of the Automatic Update policies (available in Computer Configuration\Administrative Templates\Windows Components\Windows Update):

Policy	Description
Configure Automatic Updates	Configures how automatic updates are applied on the system. Options are: • Notify for download and notify for install • Auto download and notify for install • Auto download and schedule the install (when this option is selected, configure the schedule of when to apply updates) • Allow local admin to choose setting If this policy is disabled, then automatic updates are not used, and users must go to the Windows Update website and manually install updates.
Specify intranet Microsoft Update service location	By default, clients download updates directly from the Microsoft Web site. With this policy, you identify an alternate server from which updates are downloaded. When you configure this policy, you supply two server paths:

	• Identify the server that the client will use to check for updates. • Identify the server that the client will use for logging of update status. You can also set logging to occur on any server on the network running IIS. IIS logs are found in %Windir%\System32\Logfiles\W3svc1. Both servers can be the same.
Enable client-side targeting	Use this policy to allow client to add themselves automatically to target computer groups on the WSUS server.
Reschedule Automatic Updates Scheduled Installations	If a client machine is turned off during a scheduled installation, by default the installation occurs at the next scheduled time. However, this policy allows you to set the installation to occur between 1 and 60 minutes after the system starts up.
No Auto-Restart For Scheduled Automatic Updates and Installations	This policy allows Automatic Updates to disregard a required restart when a user is logged on. The user receives a notification about the required restart but is not required to restart the machine.
Automatic Updates detection frequency	This policy specifies the time period for clients to wait before checking for updates. If not configured, the system checks for updates every 22 hours.
Allow Automatic Updates immediate installation	This policy specifies whether Automatic Updates should automatically install certain updates that do not interrupt Windows Services nor force a restart.
Delay restart of schedule installations	This policy specifies how long Automatic Updates waits before performing a restart. If not configured, the system waits 5 minutes before restarting. This policy only applies when update installations are scheduled.
Re-prompt for restart with scheduled installations	This policy specifies how long Automatic Updates waits before prompting the user for a scheduled restart. If not configured, the system prompts every 10 minutes.

Allow non-administrators to receive update notifications	This policy allows you to deliver update notifications when a non-administrator user is logged on to the computer.
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	When enabled, the install update option will not be displayed. This means that updates will be installed during shutdown because users will be unable to choose not to install the updates.

The download and installation of updates depends on the settings you specify for the **Configure Automatic Updates** policy. Actions taken for each option are:

Download Option	**Description**
Automatic	Downloads arrive without user intervention or notification.
Notification	The system waits for a user with administrator credentials to log on before sending a notification of available update downloads via a balloon above the System Tray.
Installation Option	Description
Automatic (Scheduled)	Upon successful download, an event is registered in the system event log. When a user with local administrative privileges logs on, the user can install the updates manually any time before the scheduled installation time. At the scheduled installation time, a local administrator can cancel the installation, delaying it until the next scheduled installation. A user with non-administrator privileges receives a warning message but cannot delay update installation. If no one is logged on, the installation occurs automatically.
Notification	Upon successful download, an event is registered in the system event log. When a user with local administrative privileges logs on, the user can install the updates manually.

10.4. WSUS Targeting

Targeting is the use of groups to provide different updates based on group membership. Using groups, you can deploy updates to specific computers rather than to all computers. For example, you can use targeting to:

- Create a test group where you deploy updates to evaluate their effect on computers before you deploy them to all computers.
- Create a group to exclude updates, for example if you know that certain updates are incompatible with an application installed on some computers.

Groups are created on the WSUS server through the console. Client computers are assigned to a group using one of two methods:

- With server-side targeting, group membership is assigned through the WSUS console. You manually move computers into their corresponding groups.
- With client-side targeting, group membership is assigned by configuring registry settings on the client or through Group Policy applied to client computers.

Be aware of the following when using computer groups:

- All computers are listed under the All Computers node. This is like a default group that includes all computers from every group.
- When a client contacts WSUS for the first time, it is added to the Unassigned Computers group unless client-side targeting is being used.
- You can move computers from the Unassigned Computers group into groups that you create.
- You can create as many additional groups as you want.
- A computer can be a member of multiple groups.
- To manually move a computer to another group, right-click the computer and select **Change Membership...**.
- To configure client-side targeting:
    - In the WSUS console, go to Options and then Computers. Select the **Use Group Policy or registry settings on computers** option to tell the server to use client-side targeting.

- Configure the registry or Group Policy to deliver the computer group name. In Group Policy, edit the **Enable client-side targeting** policy to specify the group name.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

10.5. MBSA

The Microsoft Baseline Security Analyzer (MBSA) is a tool you can use to scan the local and remote computers for security compliance. The MBSA tool looks for the following operating system vulnerabilities:

- Administrative vulnerabilities, such as the guest account status, file-system type, file shares, and members of the Administrators group.
- Weak passwords (blank or weak, non-expiring)
- IIS administrative vulnerabilities, including checks of virtual directories and applications and whether or not the IIS lockdown has been run
- SQL administrative vulnerabilities
- Security updates

Be aware of the following when using MBSA:

- Download and install the MBSA tool as an application. It is not included with the Windows Server 2008/2012/2016 operating system or as a server role or feature.
- Version 2.1 is required for Vista support and version 2.3 for 7/10
- You can scan a single computer by name or IP address. You can scan a local or remote computer, or even all computers in a domain.
- The newest version requires the Windows Update Service agent software on the computer being scanned. When configuring the scan, select **Configure computers for Microsoft Update and scanning prerequisites** to automatically add the Windows Update Service agent if it is not found or is not up-to-date.
- When checking for security updates:
    - Select **Scan using assigned Windows Server Update Services (WSUS) servers only** to compare the computer with the list of approved updates on the WSUS server.
    - Select **Scan using Microsoft Update only** to compare with the list of updates from Microsoft Update.
- Run **Mbsacli.exe** to run MBSA from the command line. You can also automate running MBSA by including this program in a batch file, and then setting the batch file to run on a schedule.

- MBSA requires Internet connectivity to download the list of security vulnerabilities to scan. The **Wsusscn2.ca** file is the list of items that are checked during the scan.
- MBSA only scans for vulnerabilities that have been included in the latest MBSA update. Use the Enterprise Scan Tool (EST) to scan for vulnerabilities that are not yet detected with MBSA.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757