KEEPING WINDOWS SYSTEMS UPDATED WITH SOFTWARE UPDATE SERVICES

Oscar Marco Urbano

GSEC Practical Assignment Version 1.4b, Option 1

02/19/2004

Abstract

The purpose of this paper is to explain the Software Update Services (SUS) system that Microsoft offers in order to deal with security patches, critical updates and service packs. After an introduction to this technology I will compare this product with other commercial products available in the market. Next, the server installation will be explained, as well as its administration and configuration. The secure administration is also explained. Next, I will explain how to configure clients and after the conclusion, the references are listed.

Table Of Contents

Introduction

The necessity of maintaining Windows systems updated constantly has increased in these last years due to sophisticated worm virus, hacking tools and exploits that can take control of remote systems and run arbitrary code of the attacker choice.

In these days virus protection is not sufficient to keep systems secure from intrusions. Computer systems must be up to date with security hotfixes.

Applying security patches can prevent new virus infections and make ineffective manual attacks against well know vulnerabilities.

If we remember the Blaster virus incident, we now realize that there had not been impact if all Windows systems had been patched against the RPC vulnerability.

Microsoft Software Update Services enables you to have a Windows Update Server within you own LAN and have an automatic distribution of Windows security patches, critical updates and service packs.

Many system administrators do not want that their users download and install all of the updates that Windows Update offers. And they want to test these updates in a test environment before doing the final roll-out. With Software Update Services these administrators can choose which patches will be installed and can test them before they made available these updates to final users.

It is important to note that Software Update Services only provides support for critical updates such as security patches and Service Packs, and it is only available for Windows 2000, XP, and Server 2003.

Windows XP Service Pack 1 and 2000 Service Pack 3 have the Automatic Updates client built in. Older versions, like Windows 2000 Service Pack 2 (or lower) or Windows XP without Service Pack 1, require that this client is installed separately before they can take advantage of this service.
Client software can be downloaded from:
http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp

Overview of other products

There are other products in the market that can deal with other applications and operating systems such as Windows NT.

One of these systems is Microsoft Systems Management Server (SMS) that is a complete solution for software distribution, hardware and software inventory, … However it has a more complex installation and maintenance, and it is not free while Software Update Services is free.

Another product is Shavlik HFNetChkPro Security Patch Management (http://www.shavlik.com) which can deal with Windows NT/XP/2000/Server 2003, Microsoft Office, Microsoft Exchange, Microsoft SQL Server, etc.
Microsoft Software Update Services can not distribute Microsoft SQL Server or Microsoft Office patches for example. It can only distribute core operating system patches, Windows Media Player, Internet Explorer patches, and son on, but no other specific Microsoft applications like SQL Server or Office components.
HFNetChkPro is not free.

In http://www.winnetmag.com/Files/40710/40710.pdf you can find a table comparing some more systems like BigFix Patch Manager, Ecora Patch Manager, Service Pack Manager 2000, Patchlink Update, SysUpdate, and UpdateExpert.

Server Installation

These are the minimum hardware requirements to install a Software Update Services Server:

Pentium III 700 MHz or higher processor
512 megabytes of RAM
6 gigabytes of available hard disk space

This is the recommended configuration for supporting about 15,000 clients using one SUS server

The Server Operating System requirement is Windows 2000 Server Pack 2 (or higher) or Windows Server 2003.
It also requires IIS 5.0 or higher and Internet Explorer 5.5 or later.

It must be installed on an NTFS partition. The system partition must also be an NTFS partition.

SUS Server Software can be downloaded from:
http://www.microsoft.com/downloads/details.aspx?FamilyId=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C&displaylang=en
Current version at this time of writing is:
Software Update Services Server 1.0 with Service Pack 1.

The setup utility installs IIS Lockdown 2.0 in order to secure the SUS Server. It also installs and configures IIS URL Scanner 2.5.
If IIS Lockdown or URL Scanner have been previously installed they will not be reinstalled or modified.
Even if SUS software is uninstalled, the configuration applied by IIS Lockdown and URL Scanner is not removed.

The recommended configuration by Microsoft to run Software Update Services is to install it on a dedicated server.

To begin the installation the following steps must be followed:

-Execute the downloaded file Sus10sp1.exe to begin the installation process.

-The Welcome screen appears, click Next to continue.

-Read and accept the End User License Agreement by clicking Next.

-Choose Typical check box.

-The URL that clients will use to access the SUS server will be displayed.

-Click Install.
-The SUS administration URL will be displayed. There is also a Start Menu shorcut with this URL in Administrative Tools, Microsoft Software Update Services.

-Click Finish.

-The SUS administration Web site will be opened in Internet Explorer

Administration and Configuration of the Server

The administration is performed going with Internet Explorer to the administrative URL displayed in the installation process, or using the newly created shorcut.
Administrative rights in the SUS Server are required to access this URL.

Click Set Options in the left frame to begin configure the server.

The options that can be configured are:

-Proxy Server: you can specify a proxy server to connect to and synchronize the server with other SUS server in the Internet. This is useful for those corporations that want to control or filter Internet access by using a proxy server, and going through this proxy server is the only way to access the Internet.
If the SUS Server didn't support this proxy configuration, it would not be possible to connect to the Internet and synchronize the content with other SUS server in the Internet (For instance, with some of the Microsoft's ones).
It also supports automatic proxy server configuration which means that you do not need to specify the proxy address, port, or other settings related to proxy configuration if the proxy in your network supports this automatic discovery.
If this automatic detection option is enabled in the SUS Server, it will also detect if there is no proxy server in your network. To enable it, select the checkbox *Automatically detect proxy server settings*.
You can also enable the option *Bypass proxy server for local addresses*, and then all requests addressed to the local area network will not pass through the proxy server, only those requests addressed to the Internet will pass through the proxy server.
A username and password can also be specified if the proxy server requires this authentication to allow the clients to use it. To enable this setting, check the option *Use the following user credentials to access the proxy server* and enter the username and password in the corresponding text boxes. Additionally if your proxy server requires credentials but uses basic authentication, then you should also select the checkbox *Allow basic authentication when using proxy server*.

-Server Name: Client computers can use a NetBIOS name or a valid DNS name to locate the SUS server and download the required content.
In most environments, the client computers will be able to locate the Intranet server running SUS using the NetBIOS name of the server, and then no additional configuration is required.
Other environments may require client computers to use the DNS name to locate the SUS server. This requires the configuration of a DNS name for that server.

It is also possible to use the server IP address, but this is not recommended for environments that use DHCP (Dynamic Host Configuration Protocol) because the IP addresses in these environments are not static and every change of the server IP address means the reconfiguration of the IP address in this option of the SUS Server.
Even in environments with static IP addresses, it makes the maintenance more difficult and heavy because if the IP address has to be changed for network issues, the reconfiguration of the IP address in this option of the SUS Server is also required.
And, of course, a name is easier to remember.

-Select SUS server for synchronization: you can choose to synchronize your server with the Microsoft's ones or with other local SUS server (you can even do it by means of a manually created distribution point).

If only one server is enough to support all clients (1 server can support up to 15,000 clients with the recommend configuration detailed above) then the choice is to synchronize directly with the Microsoft's ones.

If the number of clients grows above 15,000, then more than one server will be necessary to support all the clients. In this case, one SUS Server (we can call it the main or parent server) will synchronize content with the Microsoft's servers, and the rest of the other local servers will synchronize their content with this one that is synchronizing with the Microsoft's servers. With this setup only one computer will need to connect to the Internet and download the required updates, saving bandwidth in this mode, because then rest of the servers will only need to connect to this local server in order to synchronize their content, and the approval process of the updates of these servers can be automatic making easier their administration.
The list of approved updates can flow down to child servers along with the content.
To synchronize the list of approved items along with the content, when synchronizing from a local server running SUS, select the check box *Synchronize list of approved items updated from this location (replace mode)*.
After this selection is made, the child server will synchronize the list of approved packages from the parent server during the synchronization. This operation is done by making a copy of the approved packages on the parent server and using this list on the child. The end result is that the parent and child have the same list of approved items.
When this automatic synchronization of the list of approved items is selected, you will not be able to alter the list of approved items on the child server. It will be the same as the parent. The user interface to make changes to the list of approved items on the child server will be unavailable along with the Approve button on the Approve updates page.

To synchronize content from the Microsoft.com Windows Update servers, click the option *Synchronize directly from the Microsoft Windows Update servers*.

To synchronize content from another server running SUS, click the option *Synchronize from a local Software Update Services* server. In the text box, enter the name of the server from which to synchronize.

-Maintain the updates on a Microsoft Windows Update server: the downloaded updates will remain in the Microsoft Windows Update servers, they will not be stored locally.
Client computers will connect to the local server running SUS, read the list of approved updates, and then download just the list of approved updates from the Microsoft's servers on the Internet. This option can be interesting if remote client computers do not have the opportunity to connect very often or for a long time to the corporate network. They can download only a few kilobytes of information regarding the approved updates from the corporate SUS server, and can invest the rest of the time they are connected to the Internet downloading their necessary updates.

-Save the updates to a local folder: the downloaded updates will remain in the local SUS server. With this option you can configure which languages are supported.
The recommendation is to only select the languages for which you require content. This will reduce the amount of content that you need to synchronize, saving disk space and bandwidth.
If the list of supported languages is changed, you should immediately synchronize after making this change to make sure the appropriate updates for the languages added are downloaded.
If a language is removed, any updates that were previously downloaded for that language remain. SUS does not delete updates from the server. Although these updates still exist on the server, clients from the corresponding language would not receive them unless the language was entered in the supported languages list.

If a proxy server is used and it requires authentication, then the option *Save the updates to a local Folder* must be selected. This is because the Automatic Updates client only supports proxy servers that do not require authentication and it therefore will not be able to download updates from the Microsoft's servers if it needs to go through a proxy server that requires authentication.

Click Synchronize Server in the left frame to begin download updates and security patches from the server you have selected to your SUS server. The download process can be scheduled to a specified time and date.

Once the updates are downloaded you can view the synchronization log (the option in the left frame) in order to check for errors during that process.

The next step is to approve the updates (the option in the left frame) that you want to distribute to your clients.

There are two ways to deal with approved items that have their content updated during this synchronization, and both can be configured in the page of Set Options in the left frame:

-Automatically approve new versions of previously approved updates: new versions of the same update will be automatically approved.
-Do not automatically approve new versions of previously approved updates. I will manually approve these later: new versions of the same update will not be automatically approved. They will be approved manually by the administrator. This is an interesting option to test the updates before distribution. Always is a good idea to test patches to ensure they do not break anything when they are in a production environment.

The downloaded updates can have five types of status:

-New: The update has just been downloaded and it is not yet approved.

-Approved: The update has been approved by the administrator.

-Not Approved: The update has not been approved by the administrator.

-Updated: The contents of the update have been changed during synchronization.

-Temporarily Unavailable: This happens when the associated update package file required to install the update is not available or a dependency required by the update is not available.

It is important to take into account that if an approved update has been installed and then this same update has been unapproved, the update will not be uninstalled from clients.

By clicking the Details button of each update you can view the associated cab files, the link to this cab file, the command line options, the language, the required operating system, and a Read more link to get more information about a particular update.

Securing the Administration

Only those users with local administrator rights on the SUS server can access the Administration Web.

The administration of the SUS server can also be done from a remote computer via HTTP using Internet Explorer, but the HTTP protocol transmits data in clear text over the network. It does not use any kind of encryption.

To solve this, is possible to use SSL (Secure Sockets Layer) to encrypt the data for the Web administration session.
SSL is a request / response protocol that handles public and private keys, and a digital certificate.
To enable SSL in the SUS server is needed the expedition of a certificate from a valid certification entity, and this certificate should be stored in the SUS server.
The most common certificate nowadays is the 128 bit one. It is supported from Internet Explorer 4 and above. If an older browser is used, then the encryption level is lowered to 40 bits, a level that the browser can handle.
One of the most common valid certification entities is VeriSign (http://www.verisign.com)

To request a digital certificate from Verisign and apply it, the following steps must be followed:

-Execute the Internet Information Services Administration that can be found under the Administrative Tools menu.

-Right-click on the Web site where SUS is installed and click Properties.

-Start Web Server Certificate Wizard by clicking Server Certificate on the Directory Security tab, and click Next.

-Select Create a new certificate, and click Next.

-Select Prepare the request now, but send it later, and click Next.

You will have to enter a name for the certificate and a bit length. It is recommended that this bit length is 1024 to have a reasonable security.

The checkbox for the SGC (Server Gated Cryptography) certificate can be left unchecked if there are no governmental restrictions regarding export and encryption in your country.

You will also have to enter the following company information:

-Organization Name: The registered name of the company that appears on any legal document.

-Organizational Unit: The department of the company which is requesting the digital certificate.

-Common Name: The fully qualified Internet domain name of the company.

-Country / Region: The abbreviation (two letters) of the name of the country where the web server that is requesting the certificate is located.

-State / Province: The state or province where the web server that is requesting the certificate is located.

-City / Locality: The city or locality where the web server that is requesting the certificate is located.

Once this information is entered, you will have to enter the filename where the details of the certificate will be saved.

-Click next to confirm the details of the certificate and click next again.

-Click Finish.

To submit the certificate request to Verisign, you have to navigate to http://www.verisign.com/products/site/secure/index.html and choose from either a 40 bit or 128 bit (recommended) certificate. Follow the steps in the web page to submit the request and pay online.

When you receive the certificate via email (within one week), you can install it following these steps:

-Execute the Internet Information Services Administration that can be found under the Administrative Tools menu.

-Right-click on the Web site where SUS is installed and click Properties.

-Start Web Server Certificate Wizard by clicking Server Certificate on the Directory Security tab, and click Next.

-Select Process the pending request and install the certificate, and click Next.

You will have to enter the filename of the certificate that was sent to you by Verisign within the confirmation email.

The wizard will load and process the certificate. Then, the certificate summary is displayed.

-Click Next.

-Click Finish.

The next step that should be done is to enable SSL for the directories of the SUS sever:

-Right-click the \autoupdate\administration directory in the navigation panel of the Internet Information Services Administration Console, and select Properties.

-Click Edit in Secure Communications under the Directory Security tab.

-Select Require secure channel (SSL).

-Select Require 128-bit encryption, if you have obtained this kind of digital certificate. The stronger bit length of the key, the stronger the security. However a large bit key can decrease performance.

-Click OK twice.

-Repeat these steps for the following directories:
\autoupdate\dictionaries
\Shared
\Content\EULA
\Content\RTF

If \Content\EULA and \Content\RTF do not appear it means that the SUS server has not yet performed synchronization.

After doing this, you can check that it works fine if you can navigate with Internet Explorer to https://<your_server_name>/SUSAdmin

Client Installation

The Client Operating System requirement is Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server (Service Pack 2 or higher), Windows XP Professional, Windows XP Home Edition, or Windows Server 2003.

Clients will need an updated version of Automatic Updates.
Windows XP Service Pack 1 and Windows 2000 Service Pack 3 have this updated Automatic Updates client built in.
Windows 2000 Service Pack 2 (or lower) or Windows XP without Service Pack 1, need that this updated client is installed.
The updated version of Automatic Updates Client software can be downloaded from:
http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp

A local administrator of the client machine can configure Automatic Updates by using the wizard which is found in the Control Panel, or remotely by using Group Policy or by configuring the corresponding registry entries.

The possible options that can be configured are:

-To be notified before updates are downloaded, and notified again before the downloaded updates are installed.

-Updates are downloaded automatically, and the administrator is notified before updates are installed.

-Updates are downloaded automatically and installed based on a specified schedule.

The registry settings regarding the server can be found in the following registry key:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate

WUServer

Registry Value Type: Reg_SZ

Sets the SUS server by HTTP name

WUStatusServer

Registry Value Type: Reg_SZ

Sets the SUS statistics server by HTTP name. Typically this server is the same as the before one, but it can be another computer.

The registry settings of the configuration options can be found in the following registry key:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

RescheduleWaitTime
Range: n; where n = time in minutes (1-60)
Registry value type: REG_DWORD
This is used to set the wait time between the time Automatic Updates starts and the time it begins installations whose scheduled time has passed.
If a scheduled installation is missed (For instance, the client computer was turned off) and RescheduleWaitTime is not set to a value between 1 and 60, Automatic Updates waits until the next scheduled day and time to perform the installation. If a scheduled installation is missed and RescheduleWaitTime is set to a value between 1 and 60, then Automatic Updates reschedules the installation to occur at the Automatic Updates service start time plus the number of minutes specified in RescheduleWaitTime.

NoAutoRebootWithLoggedOnUsers
Registry value type: REG_DWORD
This is used to prevent Automatic Updates from restarting the computer while users are logged on. The value must be either 0 (false) or 1 (true). If this value is changed while the computer is in a restart pending state, it will not take effect until the next time an update requires a restart.

NoAutoUpdate
Range = 0|1.
0 = Automatic Updates is enabled (default)
1 = Automatic Updates is disabled.
Registry Value Type: Reg_DWORD
This is used to enable or disable the Automatic Updates feature.

AUOptions
Range = 2|3|4.
2 = notify of download and installation
3 = automatically download and notify of installation
4 = automatic download and scheduled installation.
All these options notify the local administrator.
Registry Value Type: Reg_DWORD
This is used to control the behaviour of the downloading and installation process. It can ask you before doing anything or do it automatically.

ScheduledInstallDay
Range = 0|1|2|3|4|5|6|7.
0 = Every day
1 through 7 = the days of the week from Sunday (1) to Saturday (7).
Registry Value Type: Reg_DWORD
This is used to set the day of the week for the scheduled installations.

ScheduledInstallTime
Range = n; where n = the time of day in 24-hour format (0-23).
Registry Value Type: Reg_DWORD
This is used to set the time for the scheduled installations.

UseWUServer
Registry Value Type: Reg_DWORD
If this is set to 1, then the Automatic Updates client will use the service provided by the server running Software Update Services which is specified in the registry key WUServer

These registry settings can be configured centrally using Active Directory or directly on a client computer by using the Local Group Policy Object.

The following steps are necessary to load these policy or registry settings using the Local Group Policy Object:

-Click Start, and then click Run.

-Type GPEDIT.msc to load the Group Policy snap-in.

-Under Computer Configuration, right-click Administrative Templates.

-Click Add/Remove Templates, and then click Add.

-Enter the name of the Automatic Updates ADM file: %windir%\inf\WUAU.adm

WUAU.adm is automatically installed into the %windir%\inf directory when you install Automatic Updates.

It can also be downloaded from:
http://www.microsoft.com/downloads/details.aspx?FamilyId=D26A0AEA-D274-42E6-8025-8C667B4C94E9&displaylang=en

It is also available on the server running SUS in the %windir%\inf directory.

-Click Open, and then click Close to load the wuau.adm file.

Once it is loaded, you will be able to configure policy settings for Automatic Updates with a graphical interface.

These following steps are necessary to load these policy or registry settings using Group Policy in Active Directory:

To load policy settings you will need the WUAU.adm described before.

-On an Active Directory domain controller, click Start, and then click Run.

-Type DSA.msc to load the Active Directory Users and Computers snap-in.

-Right-click the Organizational Unit (OU) or domain where you want to create the policy, and then click Properties.

-Click the Group Policy tab, and then click New.

-Type a name for the policy, and then click Edit. The Group Policy Object Editor will show up.

-Under either Computer Settings or User Settings, right-click Administrative Templates.

-Click Add/Remove Templates, and then click Add.
-Enter the name of the Automatic Updates ADM file: %windir%\inf\WUAU.adm

-Click Open.

If your organization uses Active Directory, this is the best way to deploy this policy to all the users of your domain.

The clients will query the server for new updates approximately every 22 hours. If they get a result of new updates, they will begin to download them.

The download process uses the Background Intelligent Transfer Service (BITS) to perform the download by using idle network bandwidth. If Automatic Updates is configured to notify the user of updates that are ready to download, it sends the notification to the system event log and to a logged-on administrator of the computer. If no administrator is logged on, Automatic Updates waits for a user with administrator rights to log on before offering the notification

If Automatic Updates is configured to notify the administrative user of updates that are ready to install, the notification is sent to the system event log and to the notification area in the system tray.

When a logged-on administrator clicks in the notification area icon, Automatic Updates displays the available updates to install. The administrator must then click the Install button to allow the installation to proceed. If the update requires a restart of the computer to complete the installation, a message is displayed stating that a restart is required. Until the system is restarted, Automatic Updates cannot detect any additional updates that might be applicable to the computer.

The Remind Me Later button can defers the installation. The options are: 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, tomorrow, and in 3 days.

If Automatic Updates is configured to install on a specified schedule, applicable updates are downloaded and marked as ready to install. A logged-on administrator is notified by the notification area icon, and an event is logged to the system event log. If the notification area icon is clicked, installation can be done at this time.
At the scheduled day and time, Automatic Updates installs the update and restarts the computer (if it is necessary), even if there is no local administrator logged on. If a local administrator is logged on, Automatic Updates displays a warning that an installation is about to begin. If a restart is required and a user is logged on, a similar countdown dialog box is displayed, warning all logged in users about the restart.

Conclusion

Software Update Services is a free and pretty good system to deploy critical security updates. There are other systems more powerful to do it but they are not free and are not as simple as this to use.

References

Microsoft Software Update Services:
http://www.microsoft.com/windowsserversystem/sus/default.mspx

Software Update Services Server 1.0 with Service Pack 1:
http://www.microsoft.com/downloads/details.aspx?FamilyId=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C&displaylang=en

Software Update Services 1.0 ADM File for Service Pack 1:
http://www.microsoft.com/downloads/details.aspx?FamilyId=D26A0AEA-D274-42E6-8025-8C667B4C94E9&displaylang=en

Software Update Services Client Download:
http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp

Software Update Services Deployment White Paper:
http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx

Software Update Services SP1 Release Notes:
http://www.microsoft.com/windows2000/windowsupdate/sus/sp1relnotes.asp

Microsoft Windows Update:
http://windowsupdate.microsoft.com

Microsoft Security Site:
http://www.microsoft.com/security/

Microsoft Systems Management Server:
http://www.microsoft.com/smserver/default.asp

SUSServer – Helping you update your Microsoft Windows computers:
http://www.susserver.com

Shavlik - Home of HFNetChkPro:
http://www.shavlik.com

Windows & .NET Magazine - Enterprise Patch Management for Windows
http://www.winnetmag.com/Windows/Article/ArticleID/40710/40710.html
http://www.winnetmag.com/Files/40710/40710.pdf

VeriSign, Inc.
http://www.verisign.com

VeriSign SSL Certificates
http://www.verisign.com/products/site/secure/index.html

Dev Articles – Secure Your Web Server With SSL:
http://www.devarticles.com/c/a/IIS/Secure-Your-Web-Server-With-SSL/