Global Information Assurance Certification Paper

Name: Patrick Harbauer
Version Number: 1.4
Title: Microsoft Software Update Services

Abstract

This paper will discuss Microsoft's Software Update Services (SUS) client and server software that is designed to help administrators automate the task of keeping their systems patched properly. On the server side, installation, configuration and administration will be covered. Options for SUS server placement will also be discussed. On the client side, installation and configuration will be discussed.

Version 1 of SUS is useful in many situations but does have some drawbacks that may leave administrators with no choice but to use a different tool such as SMS to deploy patches. These limitations include forced reboots, issues with server farms, mobile computing, lack of granularity when approving update packages and the fact that only critical updates, security rollups and critical security hot fixes are provided by SUS. Future versions of SUS may prove to be more functional and useful.

Overview

The need for a tool to help administrators with the tedious task of keeping Windows systems patched was made evident when Code Red hit the Internet. Firewalls and virus-scanning software alone are not enough to protect corporations from malicious code. The flawed code must be patched to fix the problem. [1]

Software Update Services (SUS) is one in a line of security tools freely available from Microsoft. SUS was developed as part of Microsoft's Strategic Technology Protection Program (STPP). Microsoft developed SUS so that administrators can bring the technology of Windows Update into their organization. SUS is targeted at medium-sized organizations to help them manage the distribution of software updates.

SUS consists of both server and client software. The server component runs on either an IIS 5.0 or .NET server (when .NET becomes available). Only English and Japanese versions of SUS are available at this time. Client systems use a special version of Automatic Updates that uses http to pull updates from the update server.

The SUS server interface lets administrators control how and when updates are deployed to client systems. Administrators also have the option to take advantage of the update servers that Microsoft has deployed around the world if their client computers are geographically dispersed. This is accomplished by using an internal SUS server to simply tell client computers which update packages to install. The client computers can then pull the updates directly from Microsoft.

Clients are supported on Microsoft Windows 2000 Professional, Server, Advanced Server (each with Service Pack 2), Microsoft Windows XP Professional, Home Edition, and the Microsoft Windows.NET Server family (when it becomes available). The Client software is actually an "agent" service. [2] Administrators can control which server each client computer connects to and schedule when the client performs all installations of critical updates. If administrators are running Active Directory Group policy, these parameters are specified in Group Policy. If Group Policy is not in use, administrator can configure client settings through the registry.

[1] Pawlak, p. 1
[2] Pawlak, p. 3

For the first release of Software Update Services, only the following types of updates are supported:

- Windows critical updates
- Windows security roll-ups
- Critical security patches

It must be stressed that ONLY CRITICAL security patches as designated by Microsoft are included.

Microsoft has guidelines for deploying SUS as follows: Administrators who already use SMS 2.0 or Group Policy to handle the deployment of software updates should continue to do so.[3] SMS is the best solution for managing software updates if you already have it deployed. Microsoft is scheduled to release the SMS 2.0 Value Pack.[4] This will assist SMS administrators in deploying updates with the same ease that SUS provides. While Group Policy has limitations as compared to SMS, if you already use Group Policy to manage software updates, Microsoft recommends that you continue to do so.

But, for administrators who manage a medium-size network and do not have an existing update solution such as SMS, Microsoft recommends SUS. [5] For administrators running Active Directory (discussed later), Group Policy can be put to great use in making SUS an even better tool. However, Active Directory is not required to use SUS effectively.

Typically, one SUS server with Internet access pulls update information directly from Microsoft. Client machines running Automatic Updates (both servers and desktops) can then pull the updates that administrators have approved. Clients pull the update(s) from the server that the administrator has specified in the client software configuration. SUS is very flexible and allows administrators to use several SUS servers or manually configure distribution servers to suit their needs. Please see the SUS deployment guide at http://www.microsoft.com/smserver/docs/sst2D.doc for full details. A sample SUS design is discussed at the end of this paper.

SUS SA Edition Beta

Microsoft has a new version of SUS in Beta called SUS SA Edition. SUS SA Edition offers the same content as the free version of SUS, but adds support for Service Packs and recommended QFE's. If you have Microsoft Software Assurance, and you would like to try to get on the Beta program, you can send an e-mail to satek-fb@microsoft.com with your request.

[3] Balian, p. 1
[4] Bekker, p. 1
[5] Davidson, p 1.

SUS Server

Pre-installation Notes

There are several items that administrators should be aware of before installing the server portion of SUS.

Application Compatibility Issues [6]

Although it is not a requirement, it is recommended that Software Update Services run on a dedicated server. If you plan to run software other than SUS on a server, please keep the following compatibility issues in mind:

- When SUS server is installed on an IIS 5.0 server (details discussed below), some applications that rely on IIS may not work properly. This is due to the fact that the SUS installation runs the IISLockDown Tool including URLScan. The version of the IISLockDown tool that comes with SUS is not customizable. It runs with no user intervention.
- Microsoft has tested the following applications and has verified that these can run on a SUS server:
    - FrontPage Server Extensions
    - SharePoint Team Services
    - ASP.NET applications
- Microsoft has verified that SUS server will **NOT** run on the following types of servers:
    - Domain Controllers [7]
    - Small Business Server 2000

[6] Microsoft, "Software Update Services Deployment White Paper", p. 11
[7] Minasi p. 1

Minimum Hardware Requirements

SUS has the following minimum hardware requirements. Microsoft states that this hardware configuration can support 15,000 clients:

- Intel X-86 or compatible P700-level processor
- 512 megabytes (MB) of RAM
- 6 gigabytes (GB) of available hard disk space

Minimum Software Requirements

The minimum software requirements for a SUS server are:

- Windows 2000 Server with Service Pack 2 or higher, or the Windows.NET Server family (when it becomes available)
- IIS 5.0 or higher
- Internet Explorer 5.5 or later
- SUS must be installed on an NTFS partition
- The server system partition must on an NTFS partition

If these software requirements are not met, the installation will fail.

IIS Installation and Configuration

Only a minimum configuration of IIS is required. The only components needed are:

- Common Files
- Internet Information Services Snap-In
- World Wide Web Server

IIS should be installed with these minimum components prior to the installation of SUS.

Installation

The server portion of SUS can be downloaded from http://www.microsoft.com/Windows2000/downloads/recommended/susserver/default.asp

A Windows Installer package is used to install SUS. The MSI file installs the required server files and pre-configures IIS in a safe fashion by running the IISLockDown Tool. The IIS Lockdown tool will reportedly not run during .NET installations. Setup does make one change to allow ASP pages to run.

Core Features [8]

Web-Based Administrative Interface

All configuration and administration for a SUS server is done using Internet Explorer 5.5 or higher. Currently only one server can be managed at a time, but administrators can manage SUS servers either locally or remotely. When logged on locally to a SUS server, only administrators are allowed to access the administrative pages.

By default, remote administration uses the HTTP protocol. This is not recommended since all HTTP traffic is clear-text. It would be possible for an internal intruder or disgruntle employee to sniff the local network and capture the username and password during logon. This could lead to the intruder logging on to the SUS server remotely and reconfiguring the server so that SUS clients download the wrong update packages. It is recommended that each virtual web site used to administer an instance of SUS be configured to allow HTTPS only.

Automated Content Synchronization and Digital Certificates

A SUS server is updated with the latest available update packages by comparing its local list of updates with either a Microsoft Windows Update server or another SUS server on the corporate intranet. Each SUS server can be configured to check for new updates either automatically at a scheduled time or manually.

There is no authentication between a SUS server and the Microsoft Windows Update servers. However, each update on the Microsoft update servers has a Microsoft digital certificate. The SUS server checks the certificate for each download and if the certificate is not a valid Microsoft certificate, the download is deleted.

Approval/Disapproval of New Updates

After new updates have been downloaded to a SUS server, they are not automatically made available to Automatic Updates clients. The SUS administrator controls which updates are available for download by approving or disapproving them individually. This is important because some updates or patches may not be compatible with a particular computing environment. There have also been problems in the past with updates fixing one or more bugs or security vulnerabilities only to introduce new bugs or vulnerabilities.[9] The

[8] Microsoft, "Software Update Services Overview White Paper", p. 7
[9] Fisher, p. 1

approval/disapproval functionality provides a mechanism to let administrators decide if and when an update is deployed.

Flexible Server Deployment and Client Configuration Options

For a small network, one SUS server may be sufficient to service all Automatic Update clients. For larger networks it may be desirable to deploy multiple SUS servers to share the load or to conserve bandwidth on WAN links.

If multiple SUS servers are required, they can be deployed in a classic parent-child configuration in which one or more child SUS servers pull their update information from a parent SUS server. All child and parent servers would be on the company's private corporate network. A very important advantage of the parent-child design is that it gives administrators the flexibility to test updates before they are deployed to production servers and desktops (discussed in more detail later in this document). With this level of flexibility, administrators can deploy several SUS servers while still limiting Internet access to one server [10].

Another option available is to configure Automatic Update clients to download updates directly from Microsoft. This option is helpful when administrators manage server and desktop systems dispersed throughout several locations and do not have the resources to place SUS servers in each office or region. Administrator can still download updates, test them and approve updates once they have been tested. One drawback to this model is that all Automatic Update clients require Internet access.

[10] Chernicoff, p. 1

Administration

The administrative interface for SUS is accessed locally by clicking on **Start->Programs->Administrative Tools->Microsoft Software Update Services**. This will launch IE 5.5 to the URL http://sus/SUSAdmin. To administer SUS remotely from the internal network, administrators can point their browser to http://<sus_server_name>/susadmin.

There is a left windowpane and right windowpane in the administrative interface. The left windowpane displays various options available for server administration. By clicking on an option in the left windowpane, the corresponding menu items or information is displayed in the right windowpane.

Welcome

The first option is the **Welcome** screen. This is a screen that displays recent news from Microsoft regarding SUS. This information is dynamic.

Synchronize server

The second option is **Synchronize server**. This screen shows the administrator the last time the SUS server was synchronized with the server it is configured to synchronize with. If a synchronization schedule is not set, **Next Synchronization** will read (None). There are also two buttons on this page – **Synchronize Now** and **Synchronization Schedule.** The **Synchronize Now** button is used for manual synchronization. The **Synchronization Schedule** button lets the administrator set a time for the server to automatically synchronize. After clicking on the **Synchronization Schedule** button, the Schedule Synchronization dialog appears. Once the **Synchronize using this schedule** radio button is selected, the available options are to set synchronization to a specific hour in the day and to select either **Daily** or **Weekly** synchronization. If **Weekly** synchronization is selected, the administrator chooses a day of the week. The only other option for synchronization is to set the number of times SUS retries synchronization if previous attempts have failed. Retries can be set between 0 and 100.

Approve Updates

The third option is **Approve Updates**. This is where the administrator can view all updates that have been downloaded to the local SUS server and the status of each update. The status for an update will be one of the following:

- **New**: A completely new update that was downloaded the last time the SUS server synchronized content with the designated server.
- **Not Approved**: An update that the administrator has explicitly chosen not to approve.
- **Updated**: An update that was previously approved but has been revised by Microsoft.
- **Approved**: Updates that the administrator has approved for download to client machines.
- **Temporarily Unavailable**: Updates that failed to download, or one or more other updates are not available that this particular update must be installed with.

To approve new updates, administrators simply scroll through the list of updates, select the checkbox to the left of each update that they wish to approve and then click on the **Approve** button located on the bottom-right-hand corner of the screen.

To disapprove updates, administrators deselect the checkbox to the left of each update that they wish to disapprove and then click the **Approve** button.

If an update was previously approved and then the administrator later decides to disapprove it, SUS has no capability to remove the update from clients that have already downloaded the update. Disapproving an update only prevents additional clients from downloading that particular update.

If the administrator has configured the SUS server so that updated patches must be manually approved, some patches will be labeled **Updated**. These are updates that have been previously released but have been updated by Microsoft to correct a shortcoming of the previous release of the update.

Each individual update displays the following information:

- A descriptive title (sometimes including the date the update was released).
- The date the SUS server downloaded the update.
- The download size.
- A short description stating what the update is for.
- A **Details…** hyperlink that opens a dialog box showing the following:
    - Platform – This shows the operating system(s) that the update is for.
    - Locale – This shows the locale for the update (English, Japanese, German, etc.).
    - Date – The date the SUS server downloaded the update.

    - Size – The size of the update file.
    - Setup Parameters – Parameters used to manually run the update.
    - Info – This opens yet another dialog box that gives further details about the update. A link is also provided to the Microsoft Q article that discusses the update.
    - File Name – The name of the executable to install the update.
- If the installation of the update requires a reboot, it will be noted in red letters stating, "Installation requires a reboot".
- The Operating System(s) that the update applies to.

Notes About Approvals

- There is a timing issue to be aware of. Client computers running Automatic Updates poll the SUS server every 22 hours minus a random offset. So be aware that updates that are approved are not installed immediately.
- Dependent updates must be approved/disapproved together. If an administrator attempts to approve or disapprove an update that has dependencies, detailed information is displayed explaining the other updates that are dependent. If the administrator decides to go ahead and approve/disapprove the package, all dependent packages are also approved/disapproved.
- All approvals and disapprovals are logged.
- One drawback to SUS is that it does not allow administrators to group update packages for a particular group of servers and workstations. All packages approved on a SUS server are available to all client systems configured to use that particular SUS server. [11]

Other Options

View Synchronization Log, **View approval log**, **Set options** and **Monitor server** are available under the **Other Options** subheading.

View Synchronization log

The Synchronization log provides details about synchronization sessions that have taken place between the local SUS server and the server that it is configured to synchronize with. This log shows the time that a manual or scheduled synchronization started, details on the updates added, updates removed, reissued updates and any errors that may have occurred. If no updates were available, the log states that SUS was up to date at the time of the synchronization. There are two buttons at the bottom-right-hand corner of the View Synchronization log screen – **Clear Log** and **Print Log…**

[11] Pawlak, p. 2

View Approval log

This log provides details showing the time and date that the approved list was last modified, whether or not the approval process was successful or unsuccessful and the user who performed the approval. Each individual update is then listed under the categories of Approved Updates, Unapproved Updates and New Updates. There are two buttons at the bottom-right-hand corner of the View Approval log screen – **Clear Log** and **Print Log…**

Set Options

This menu item displays several options that the administrator can set for the SUS server.

Select a proxy server configuration

If a proxy is used, the administrator can select to either let SUS automatically detect proxy server settings or the administrator can manually set the proxy server settings. Settings are available to designate the IP address and port number of the proxy server, a username and password and whether or not to allow basic authentication when connecting to the proxy server.

Specify the name your clients use to locate this update server

This field is used to specify the NetBIOS name clients should use to connect to the local SUS server. If for some reason your clients will not be able to use the NetBIOS name of the SUS server to locate it, the administrator should designate the DNS name of the SUS server.

Select which server to synchronize content from

This field is used to let the administrator specify which server the local SUS server uses to synchronize. The two options are:

- **Synchronize Directly from the Microsoft Windows Update servers**
- **Synchronize from a local Software Update Services server**
    - If this option is selected, the administrator enters the name of the SUS server that they would like the local server to synchronize with. If this option is selected, the administrator has the option to select the **Synchronize list of approved items updated from this location (replace mode).** If this is selected, the list of approved updates will be replaced every time the server synchronizes with the designated synchronization server.

Select how you want to handle new versions of previously approved updates

The two options are:

- **Automatically approve new versions of previously approved updates.** If this is selected, clients will automatically download new versions of updates the next time they check the server for updates. No administrator interaction is required.
- **Do not automatically approve new versions of approved updates. I will manually approve these updates later.** If this option is selected, the administrator must manually approve revised updates before clients can download them.

Select where you want to store updates.

The two options are:

- **Maintain the updates on a Microsoft Windows Update server**. If this is selected, only the metadata files are downloaded from Microsoft. The client machines running Automatic Updates pull the update packages directly from the Microsoft Windows Update Servers. Metadata describes the details of each update package. Details include information such as which OS or application the update applies to, the size of the update package and whether a reboot is required. Metadata is saved in the AUCatalog.cab file.
- **Save the updates to a local folder**. If this is selected, the metadata and the update files are downloaded to the local SUS server.

Synchronize installation packages only for these locales

- This is where the administrator designates which locales are required for her network. Thirty-one locales were available at the time of this writing. The administrator should only select the required locales to save disk space. Two buttons are available in this section: **Select All** and **Clear All**.

Monitor Server

To improve the performance of SUS, the list of available updates for each application and OS platform available are cached. Available applications are IE 5.0X, IE 5.5X and IE 6.X. Available OS platforms are Windows 2000 and Windows XP. The caches are populated with items.txt files stored in the //sus/dictionaries/autoupdate folder. There is one folder and items.txt file for each application and OS. If the date and time displayed in the **Most Recent Update** column is not in-synch with the last synchronization, click on the **Refresh** button to repopulate the cache.

See Also

The menu options under the **See Also** subheading are **About Software Update Services**, **Microsoft Windows Update**, **Microsoft Security** and **Microsoft Support Knowledge Base**. These are all good resources for learning more about SUS and security in general.

SUS Client – Windows Automatic Updates

SUS requires a special version of Automatic Updates that is based on the Automatic Updates client shipped with Windows XP. The client currently runs on Windows 2000 Professional, Windows 2000 Server, and Windows 2000 Advanced Server (Service Pack 2 or higher). It also runs on Windows XP Professional and Windows XP Home Edition. [12]

The client portion can be downloaded from http://www.microsoft.com/Windows2000/downloads/recommended/susclient/default.asp

Installation

The installation method used can be the same method that the administrator currently uses to deploy new software. Some possibilities are going to each computer and running the installation program manually, pushing the client software out to the client machines using SMS or Group Policy or using a logon script.

Core Features [13]

The SUS client has been secured so that only a local administrator can access it. This prevents standard users from changing the client settings. If Active Directory is used to configure the client, then all options in the Automatic Updates control panel are disabled. Not even the local administrator has access. Only the Domain Administrator can make changes to the client settings.

To confirm that packages have not been tampered with, the Automatic Updates client makes sure that Microsoft has digitally signed each package and does a CRC check on each package before downloading it.

If multiple updates are installed simultaneously and one or more of them requires a reboot, the SUS client automatically uses the Microsoft QCHAIN utility to ensure that all packages are installed properly.

[12] Microsoft, "Software Update Services Overview White Paper", p. 11
[13] Microsoft, "Software Update Services Overview White Paper", p. 7

Administration

There are three possible ways to configure SUS clients:

1) Manually configuring each client system.
2) Configuring each client system through the registry using system policies.
3) Configuring each client using Active Directory Group Policy.

Options two and three will be discussed here.

Client Configuration using System Policies

If Active Directory Group Policy is not an option (for example, all domain controllers are Windows NT 4.0) system policies can be used. A policy with the following registry settings can be used.

Registry Settings [14]

This group of settings is stored in HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

- NoAutoUpdate
  Range = 0|1. 0 = Automatic Updates is enabled (default), 1= Automatic Updates is disabled.

- AUOptions
  Range = 2|3|4. 2 = notify of download and installation, 3 = auto download and notify of installation, and 4 = auto download and scheduled installation. All options notify the local administrator.

- 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).

- ScheduledInstallTime
  Range = n; where n = the time of day in 24-hour format (0-23).

- UseWUServer
  Set this to 1 to enable Automatic Updates to use the Software Update Services server as specified in the **WUServer** value.

[14] Microsoft, "Software Update Services Deployment White Paper", p. 62

This group of settings is stored in HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate. These keys specify which server your SUS clients use to retrieve updates and where to send statistics:

- WUServer
  Sets the Windows Update intranet server by HTTP name (for example, http://updatedownloads).
- WUStatusServer
  Sets the Windows Update intranet statistics server by HTTP name (for example, http://updatestats).

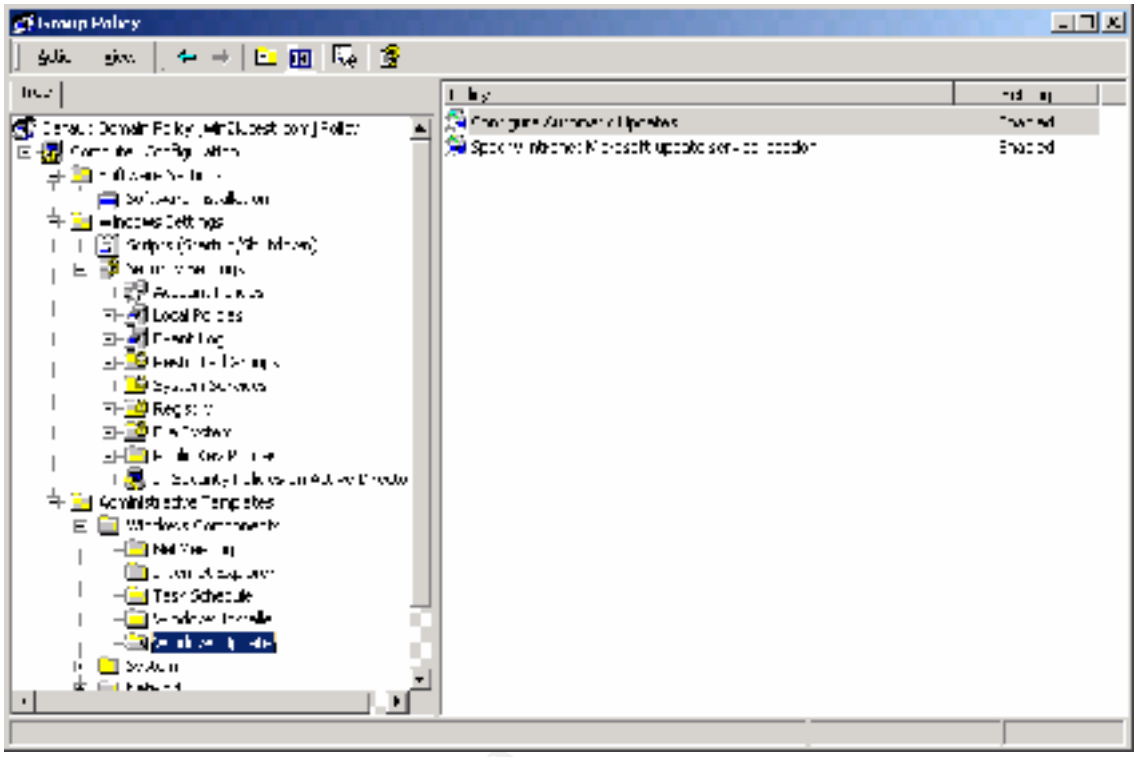
Client Configuration using Active Directory Group Policy [15]

If Active Directory is deployed, Group Policy can be used to configure SUS clients. Group Policy settings always override local user-defined options. When Group Policy has been defined, the Automatic Updates control panel options are disabled on client systems.

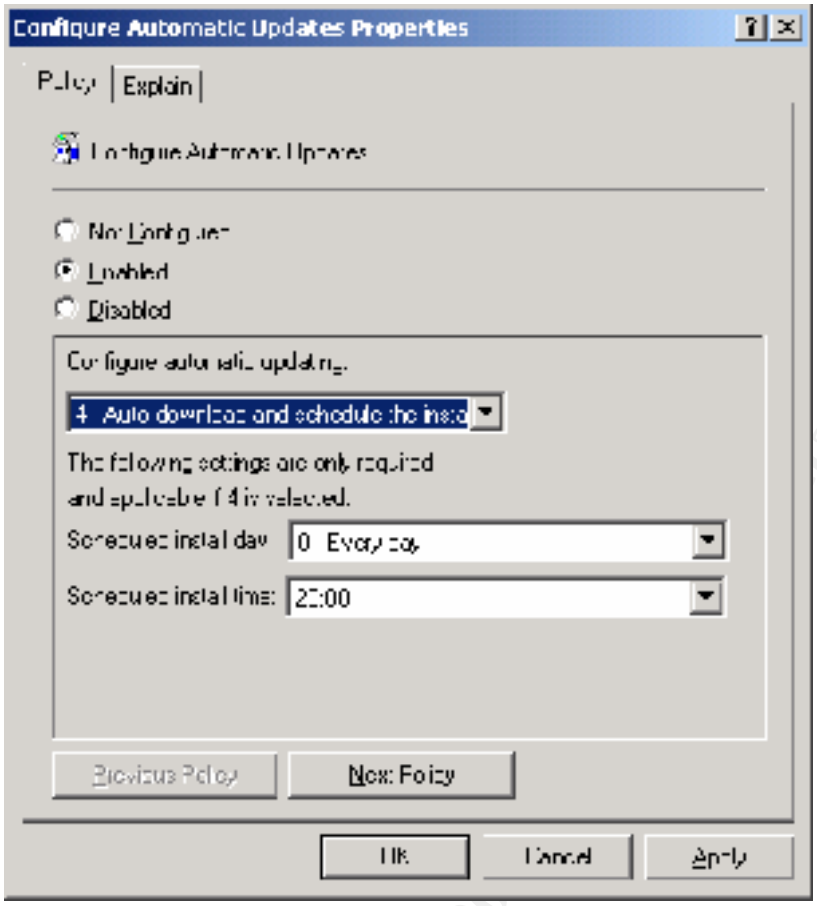
There are two Group Policy settings pertaining to SUS clients under **Computer Configuration->Administrative Templates->Windows Components->Windows Update**. There is one Group Policy setting pertaining to SUS clients under **User Configuration->Administrative Templates->Windows Components->Windows Update**.

[15] Microsoft, "Software Update Services Deployment White Paper", p. 59

The two Policies under **Computer Configuration** are **Configure Automatic Updates** and **Specify intranet Microsoft update service location**.



Configure Automatic Updates



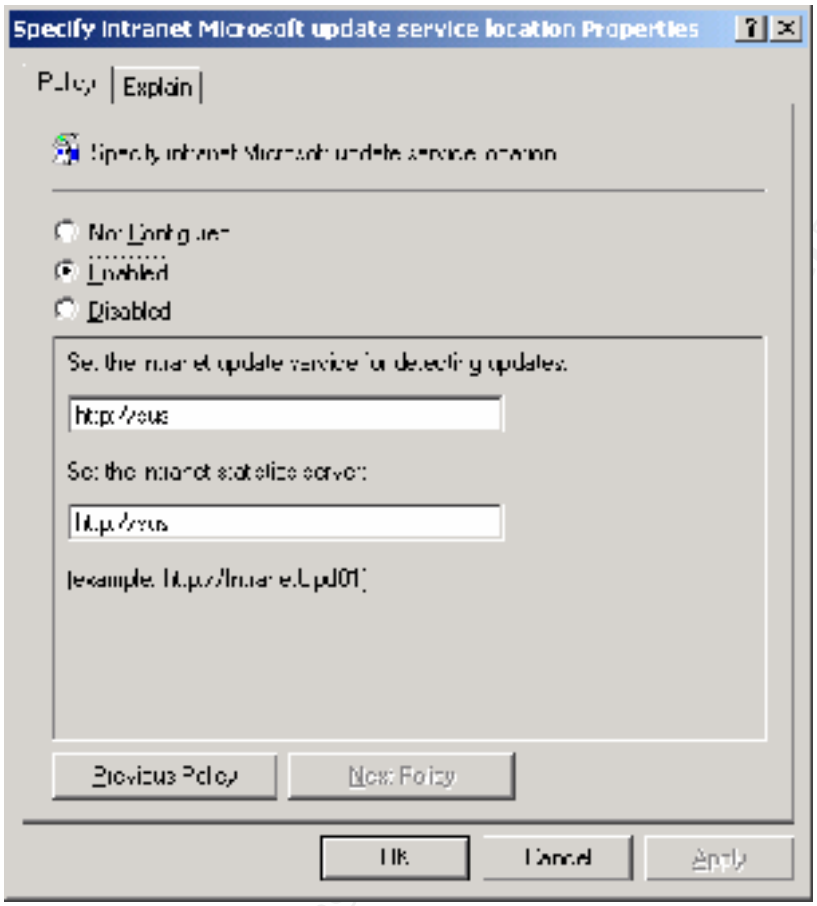
As with all policies, this policy can be set to **Not Configured**, **Enabled** or **Disabled**. If this policy is disabled, no updating will occur automatically.

Under **Configure Automatic Updating**, there are three options:

1) Notify for download and notify for install – If an administrator is logged on, she will be notified before updates are downloaded and before downloads are installed. If an administrator is not logged on, Automatic Updates waits for an administrator to log on before displaying any notifications about downloading and installing updates. Updates are downloaded and installed once an administrator has chosen to do so.
2) Auto download and notify for install –Updates are downloaded with no notification, but if an administrator is logged on, she will be notified before installation of updates. If no administrator is logged on, Automatic Updates waits for an administrator to log on before displaying a notification that downloads are available for install. Updates are installed once an administrator has chosen to do so. This setting is the default.
3) Auto download and schedule the install – If no user is logged on, the updates are automatically downloaded and installed and the computer is rebooted if necessary. If an administrator is logged on when downloads are ready for installation, the administrator is given the option whether or

not to install the updates. If the updates are installed and require a reboot, the administrator is given the option whether or not to reboot. If this updating option is selected, the SUS administrator specifies the day and time that installs occur.

Specify intranet Microsoft update service location



The parameters that can be set for this policy are **Set the intranet update service for detecting updates** and **Set the intranet statistics server**. The **Set the intranet update service for detecting** updates parameter can be set to either a server running SUS or an IIS server that has been configured as a Manual Content Distribution Point. Manual Content Distribution Points are discussed later in this document. Setting this parameter determines which server a client polls for new updates and which server it downloads updates from.

The **Set the intranet statistics server** parameter points clients to the server to send download statistics to. This parameter can be set to the same server as the server that clients download updates from or another IIS server. The statistics are saved in the IIS Logs format.

Policy templates

When SUS is installed, a policy template file named Wuau.adm is included. These policies will also be included in the System.adm file in Windows 2000 Service Pack 3, with the Windows.NET Server family, and with Windows XP Service Pack 1 when they are made available.

For full details to enable Windows Update Group Policy, see pages 56 through 59 of “Software Update Services Deployment White Paper” at http://www.microsoft.com/windows2000/windowsupdate/sus/susdeployment.asp.

Sample SUS Design

This sample deployment is designed to allow an administrator to fully test update packages before they are deployed to production servers and desktop computers. One SUS server and one Manual Content Distribution Point are required for this design. The SUS server (we will name it TEST) is configured to download all updates automatically from the Microsoft Windows Update servers. The other server (DEPLOY) is a Manual Content Distribution Point. Test servers and desktop computers are used to verify that each update package can be safely deployed to the production environment. All production servers and desktop computers are configured to pull update packages from DEPLOY. Figure 1 depicts this scenario and the logical flow of update packages.

Manual Content Distribution Point

A manual content distribution point is created by copying files manually from a SUS server to a server running Internet Information Server (IIS) version 5.0 or higher. SUS is not installed on a Manual Content Distribution Point. A web site is created on an IIS server and content is copied from a SUS server as explained below [16].

Procedure to Create a Manual Content Distribution Point

1. Select the server that will be used as the Manual Content Distribution Point. This can be a server with no access to the Internet. IIS 5.0 or higher must be installed.
2. Create a folder with the name \Content on the Manual Content Distribution Point server. Preferably this is not on the same drive as the Windows OS directory.
3. Copy **all** of the following files and folders from the SUS server to the \Content folder on the Manual Content Distribution Point:
    - <root of the SUS Web site>\Aucatalog.cab
    - <root of the SUS Web site>\Aurtf.cab
    - <root of the SUS Web site>\approveditems.txt
    - all the files and folders under the \Content\cabs directory
4. Create an IIS Vroot pointing to the \Content folder.
5. Repeat step 3 each time new updates are to be made available to Windows Update clients configured to download updates from the Manual Content Distribution Point server.

[16] Microsoft, "Software Update Services Deployment White Paper", p. 27

Referring to Figure 1, TEST will pull new update information directly from the Microsoft Update Servers. This will occur either manually or at a specified time based on how the administrator has configured the server. The administrator then approves the updates on TEST that she wishes to test on the test servers and desktops. Once she has determined which updates she wishes to deploy to the production environment, she disapproves any new updates that she determined could not be rolled out to the production environment. She then updates the Manual Content Distribution Point server per the procedure outlined above. The production servers and desktops will then pull the newly approved updates from the Manual Content Distribution Point server the next time they poll it for updates.

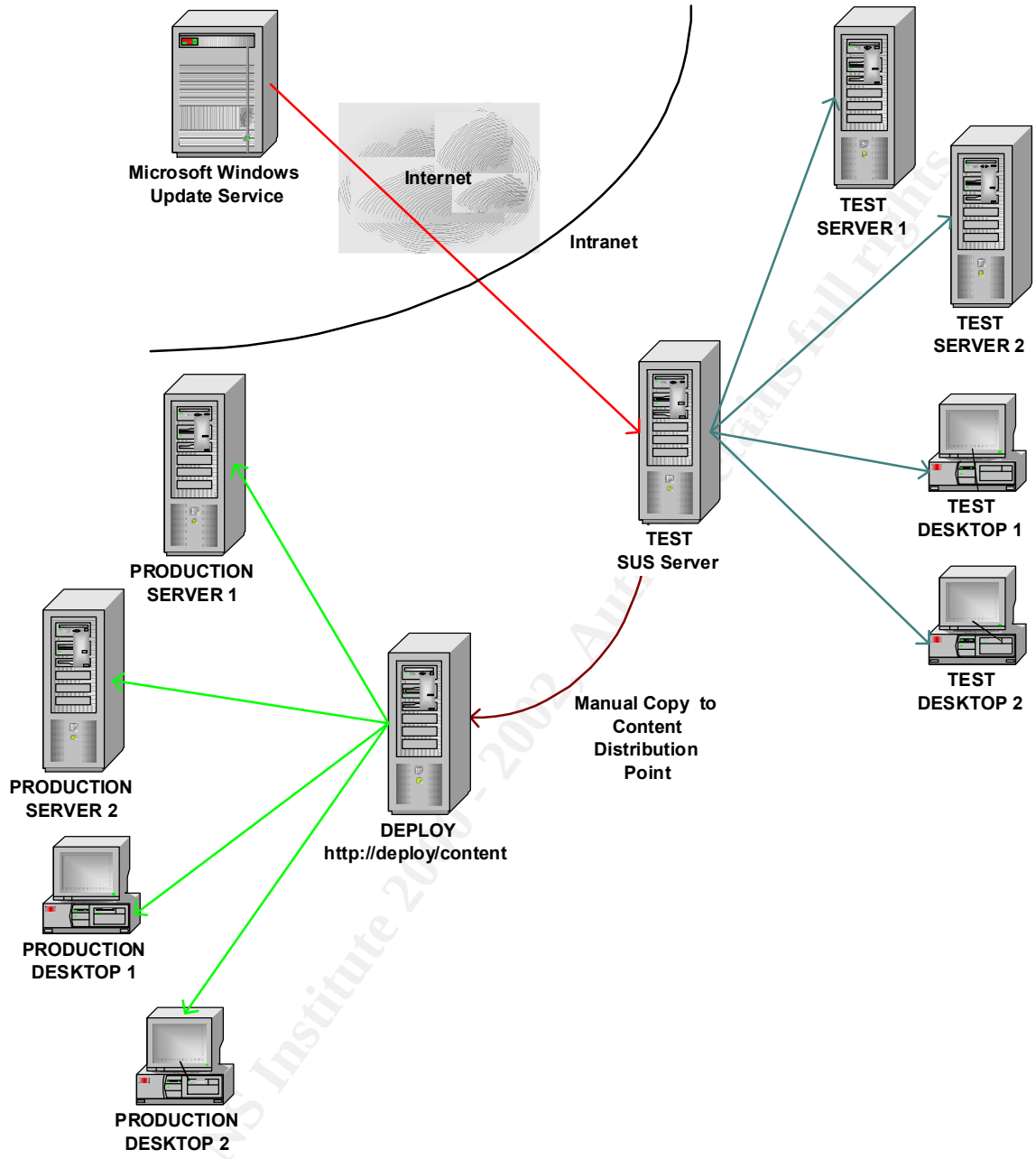


Figure 1 – Sample Manual Content Distribution Point Design

Conclusion

SUS can be a very useful tool in certain situations. The following drawbacks may make it hard for many administrators to implement SUS. [17] If these drawbacks are addressed in newer versions of SUS, SUS could become a much more powerful and useful tool.

Automatic Reboots

Certain packages will require a reboot after installation. If SUS is configured on a mission-critical server, data could be lost if an administrator is not logged on to defer the reboot. Also, users may leave their desktops logged on with an application open. If they have not saved their work, a forced reboot would cause data loss or corruption.

Server Farms

The SUS client piece does not take into account that it may be loaded on a server that is part of a server farm. If an update requires a server reboot, all servers in the farm may be down at the same time.

Does Not Address Mobile Computing

If end-users travel from office to office with their laptops, the Automatic Updates client does not determine which SUS server is closest. It will always pull updates from the same SUS server. This could have adverse effects on bandwidth utilization of a WAN.

Package Approval Not Granular

SUS does not allow administrators to group client systems to receive a specified group of update packages. Only one group of update packages can be approved for each SUS server.

Only Certain Updates Addressed

With this version of SUS, only Windows Critical Updates, Security Rollups and Critical Security patches are provided by SUS. There are other updates that tools such as Microsoft HFNETCHK will report. Unfortunately, HFNETCHK does not have any tools such as SUS for rolling out updates.

[17] Pawlak, p. 7

References

Balian, Cheryl. “Microsoft Says New Security Tool Will Routinely Patch Vulnerabilities”, 2, May 2002. URL: http://www.infosecuritymag.com/2002/may/digest02.shtml#news2 (24, Jul. 2002)

Bekker, Scott. “Microsoft Does SMS 2.0 Value Pack, Software Update Services.” 1 May 2002. URL: http://www.entmag.com/news/article.asp?EditorialsID=5334 (16 Jul. 2002).

Chernicoff, David. “Keeping Up with Updates” 16, May 2002. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=25217 (24 Jul. 2002)

Davidson, Michelle. “Microsoft makes patching easy at management summit.” 1 May 2002. URL: http://searchsystemsmanagement.techtarget.com/originalContent/0,289142,sid20_gci820733,00.html (16 Jul. 2002).

Fisher, Dennis. “Microsoft Security Tool Leaves Holes.” 22, Apr. 2002. URL: http://www.pcmag.com/article2/0,4149,27758,00.asp (16 Jul. 2002).

Microsoft, “Software Update Services Overview White Paper”, 20, Jun. 2002. URL: http://www.microsoft.com/windows2000/windowsupdate/sus/susoverview.asp (16, Jul. 2002)

Microsoft, “Software Update Services Deployment White Paper”, 20, Jun. 2002. URL: http://www.microsoft.com/windows2000/windowsupdate/sus/susdeployment.asp (16, Jul. 2002)

Minasi, Mark. “Software Update Service: Worth a Look. “2, Jul. 2002. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=25778 (24 Jul. 2002)

Pawlak, Peter. “Software Update Service to Ease Patch Distribution.” 22, Apr. 2002. URL: http://www.directionsonmicrosoft.com/sample/DOMIS/update/2002/05may/0502sustep.htm (24 Jul. 2002)

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS