

ODFT – Enterprise

Microsoft's Software Update Service

Written by Matt Capranos

Microsoft's System Update Services

Table of Contents

Notice.....	Page 3
Executive Summary.....	Page 4
Why Use Software Update Services.....	Page 5
How Does Software Updates Services Work.....	Page 7
Active Directory Integration--Using Group Policy With WUAU Policy.....	Page 11
What Software Update Services Can And Cannot Do.....	Page 13
Recommended System Requirements.....	Page 14
Future of Microsoft's Software Update Services.....	Page 15
Conclusion.....	Page 16
References.....	Page 17

Microsoft's System Update Services

Notice

This paper is being presented by ODFT-Enterprise as a discussion of Microsoft's Software Update Services. The case paper presented here is the rightful property of ODFT-Enterprise and is being produced to be reviewed by William Farkas of TELE 38525 Network Operations. The purpose of this paper is to discuss the usefulness, capabilities, brief system requirements, and active directory integration of Microsoft's Software Update Services. This paper is not to be reproduced or distributed unless the explicit permission of ODFT-Enterprise is given.

Disclaimer

Every effort is made to provide accurate and complete information. However, with the documentation available from Microsoft and additional sources that were used to complete this document are often uploaded within short deadlines, we cannot guarantee that there will be no errors. With respect to this document, ODFT-Enterprise nor their employees and contractors make any warranty, expressed or implied, including the warranties of merchantability and fitness for a particular purpose with respect to this document and the research that was performed by ODFT-Enterprise and their employees. Additionally, ODFT-Enterprise assumes no legal liability for the accuracy, completeness, or usefulness of any information, product, or process disclosed herein and does not represent that use of such information, product, or process would not infringe on privately owned rights.

Executive Summary

The purpose of this paper is to publish the research of ODFT-Enterprise's analysis of Microsoft's System Update Services. Entailed in this analysis, the usefulness, capabilities, brief system requirements, Active Directory integration of Microsoft's Software Update Services and the future of Software Update Services will be discussed. The following paper was commissioned by William Farkas of TELE 38525 Network Operations. In this discussion of Microsoft's Software Update Services the following criteria will be discussed;

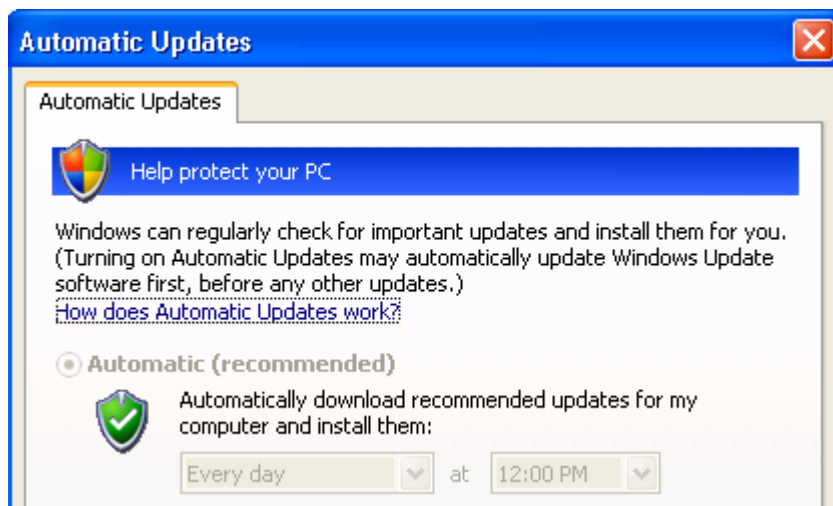
- Why use Microsoft's Software Update Services?
- How does Software Update Services work?
- Active Directory integration, using group policy objects with WUAU policy.
- What Software Update Services can and cannot do.
- Recommended system requirements.
- Future of Software Update Services.

The difficulty faced by network and system administrators is to maintain a uniformed updating schema for a Windows XP, 2000 and 2003 operating system environment. With the ever growing need to ensure that computers and servers receive the latest patches and updates to protect their systems from potential exploits and malicious attacks a uniformed updating schema is necessary. Such a schema would then increase the stability and performance of said systems and servers. In the past, administrators would have to specify the times in which updates would be downloaded and applied, and in some situations the administrators would have to go from computer to computer applying these updates.

To help combat this problem, Microsoft is now offering a new service called Software Update Services (SUS). The service allows time strapped administrators to centralize control over the method in which computers and servers receive their updates by using a combination of administrative templates, Active Directory, and group policies; administrators can choose which computers and servers will receive the updates at a time of their choosing. In the following sections of this document, several topics will be discussed in order to give a more in depth overview of what Microsoft's System Updates Service is and what it has to offer system administrators.

Why use Microsoft's Software Update Services?

Microsoft's Software Update Services is an option used by administrators to centralize the downloading of patches and security updates for Microsoft's Windows operating systems (Win XP, 2k and 2k3); and coupled with the use of Active Directory and Group Policy, administrators can direct how the updates will take place. With the ever growing problem of maintaining a uniform updating schema across an enterprise network, administrators have to spend a great deal of time and effort to ensure that the computers and servers are receiving the proper updates in order to patch potential security exploits or to help increase system stability and performance. In the past, administrators would have to go to each machine to set the Windows Update Automatic Updates (WUAU) policy to download and apply the required updates from Microsoft's Servers.



(Screen capture from Windows XP machine)

To help illustrate, the above screen shot shows the typical setting that most administrators have in place on the computers that are connected to the enterprise network. The example shows that this machine will download all new updates daily and will install them everyday at noon. While the above example does offer good coverage for this particular Windows Client, the settings ensure that new updates will be downloaded and applied daily. However, there is still a fundamental flaw with this option.

The flaw being: If there were only a few Windows computers on the network and several large updates have to be downloaded simultaneously, a small bottleneck on the WAN link can occur, but as the number of computers on the network increases as does the bottleneck. In an effort to prevent this, an administrator would have to go to each Windows computer and vary the time in which the computers would download their updates; however, this will cause an increase in administrative overhead.

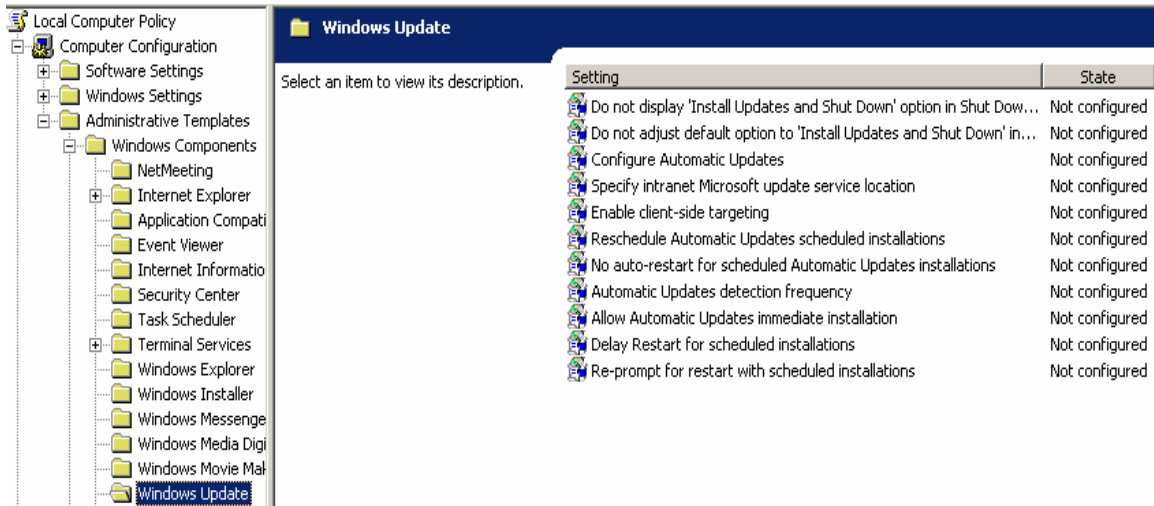
Microsoft's System Update Services

As the number of Windows computers increases, as does the administrative overhead, thus forcing administrators to setup every machine manually before sending it out to the office. This can be a time consuming experience, and if a single machine is missed it can lead to possible vulnerabilities on network.

To make it easier for administrators, Software Update Services can be configured on the corporate network to handle this daunting task. Having Software Update Services running allows administrators greater centralized control over which machines will update at which time. Indeed, there are additional benefits of running this service: such as generating reports on which machines have received updates; having Windows computers download updates from a SUS server attached to the LAN rather than using a limited WAN link; and allowing administrators to approve updates before they are sent to computers on the network.

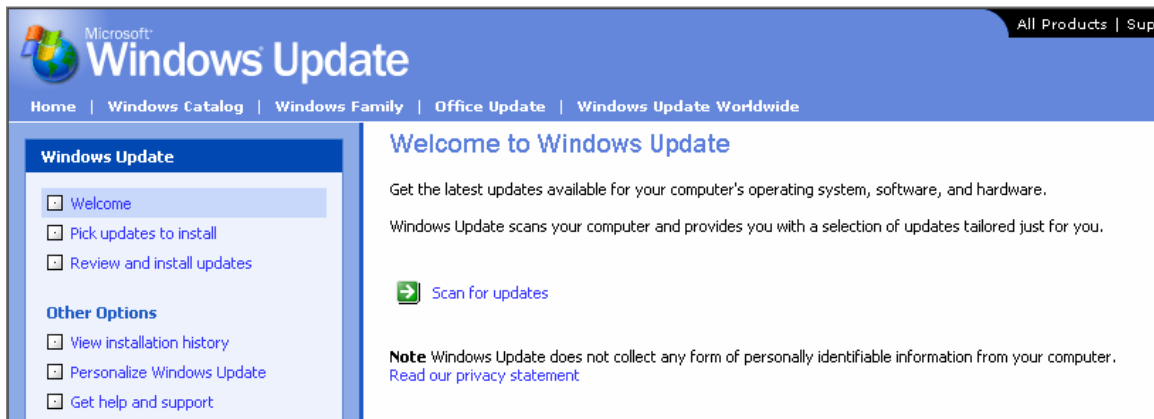
How Does Software Update Services work

Before delving further into Microsoft's Software Update Services, a quick note on how Windows computers not using SUS would download updates. There are two ways in which a Windows computer updates itself: the first as mentioned in a previous section, is to have a Windows Update Automatic Update (WUAU) policy put in place to download updates at a pre-determined time. An example of the policy is shown below.



(Windows Update Automatic Update Administrative Policy)

The second option is to have a Windows computer connect to Microsoft's Windows Update site, and use their service to scan the computer for required updates then download said updates from the Windows Update site and then install the updates on the computer.

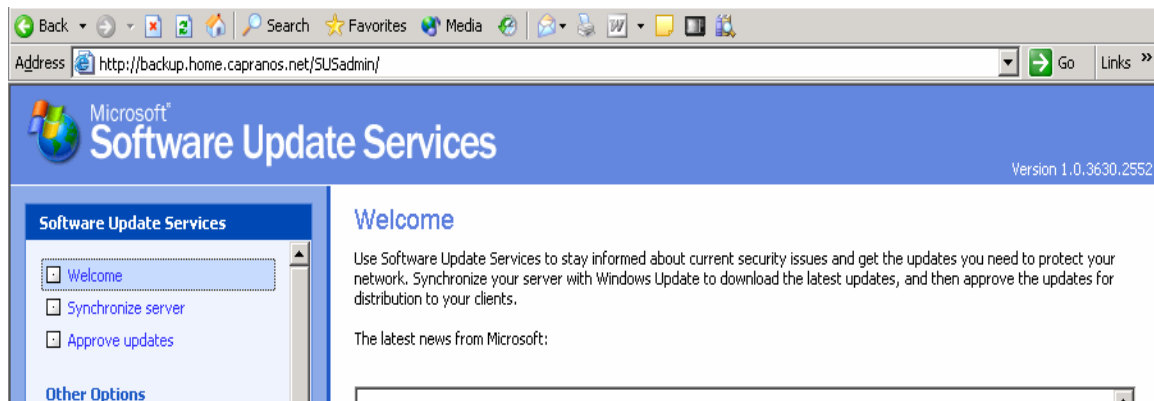


(The above screen shot is from Windows Update Site)

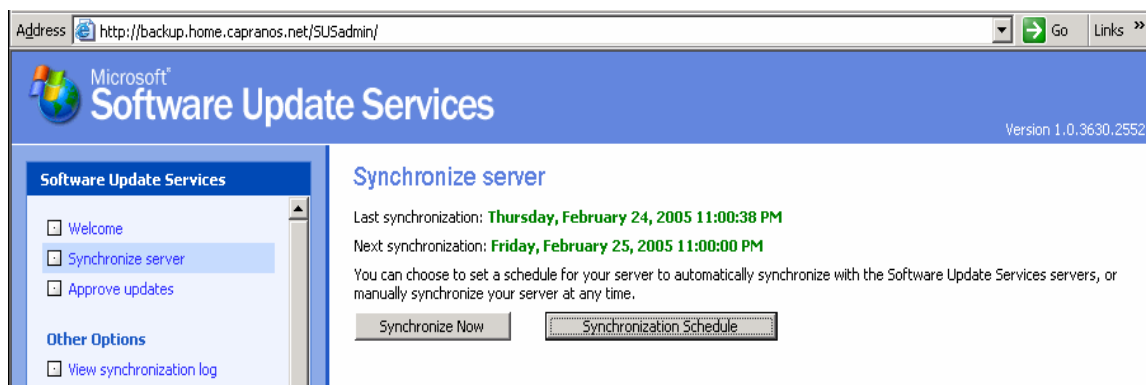
The problem with both options is the lack of flexibility. The Windows Update Automatic Update (WUAU) policy has to be put in place by an administrator while sitting at the machine. The above Windows Update website has limitations as well; only those with administrator rights can download and apply new updates.

Microsoft's System Update Services

Microsoft's SUS service incorporates the Windows Update Automatic Update (WU) policy and the Windows Update website. The WU policy schedules the time in which new Windows updates are downloaded and installed; and an installable version of the Windows update website is installed on a local network server which assists administrators in applying said updates to computers on the network. The Software Update Service is the server component, which is installed on a machine running either Windows XP Professional, 2k or 2k3, which is located within a company's internal network.



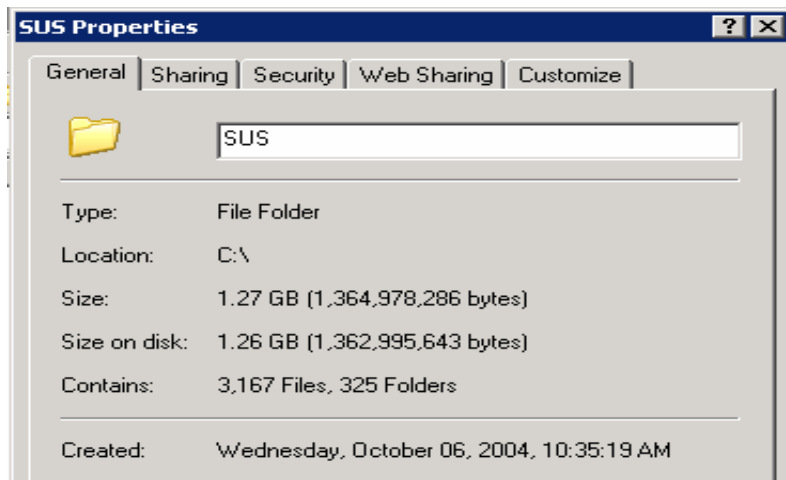
The internal SUS server has to be periodically synchronized with the Windows Update Website when new critical updates are made available. This process can be a manual procedure initiated by an administrator or a synchronization process that can be scheduled.



As new updates are made available, there are two options for administrators when it comes to where the clients will receive their updates. In SUS, administrators can have all of the Windows Updates downloaded and stored on a central server(s) on the network; the Windows computers will then connect to the SUS server to download their updates. However, having a copy of all the English only updates for Windows XP, 2000 or 2003 platforms can accumulate a great deal of space.

An example of the SUS server running on the home.capranos.net domain requires 1.27 GB of storage. A screen shot of such an example can be seen on the next page.

Microsoft's System Update Services



(The current storage requirement for SUS on the home.capranos.net network)

If available storage is at a premium on a corporate network, the second available option for administrators is to specify that computers download all newly approved updates directly from Microsoft's servers. While this option may save space, it does have a major disadvantage: if the WAN link used to connect computers is particularly slow or is on a cost per byte usage, computers using the link at the same time can create a large bottle neck, or the link may become quite expensive to use. A good example would be the release of Service Packs for Windows XP: service pack 2 is approximately 200 megabytes in size; if several hundred computers are downloading it at the same time, this could bring a corporate WAN link to a stop.

When new updates become available for use, it is then up to the administrators to approve which updates will be sent out to the computers. By approving the new updates, this will help to prevent random or undocumented problems from occurring. To assist administrators, a small test network with a separate SUS server can be configured to test new updates for potential problems. After the testing cycle is complete, administrators can then approve the updates on the live network SUS server for distribution.

Approve updates

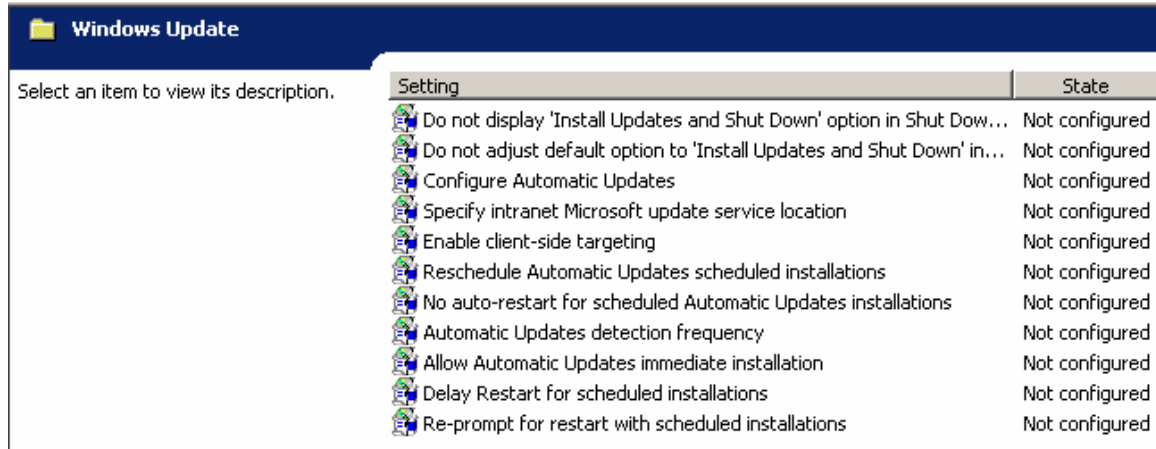
Choose the updates that you would like to distribute to your clients, and then click **Approve**.



(Screen shot of new updates, available for distribution)

Microsoft's System Update Services

Following the approval of new updates by an administrator, these updates need to be downloaded by Windows computers on the network; SUS makes use of the Windows Update Automatic Update (WUAU) policy on the Windows computers to do so. The WUAU policy is used to specify when the updates will be downloaded, where the updates will be downloaded from, and how the Windows computer will act after the new updates have been installed.



(Screen capture showing the Windows Update Automatic Update policy)

For the WUAU policy to be effective it has to be configured on Windows computers; and there are several options on how to configure this policy. The first option is to have a person with administrative permissions go to each computer and manually install the policy; doing so requires a great deal of time and the benefits of centralized control are lost. The second option is through the use of login scripts and registry values. While this will ensure all Windows computers that log on to the domain will download the update, this can be difficult and time consuming to implement by having to write separate scripts for different departments or user groups. The third option, if the corporate network is using Microsoft's Active Directory, a group policy with the WUAU policy can be configured for all Windows computers on the network.

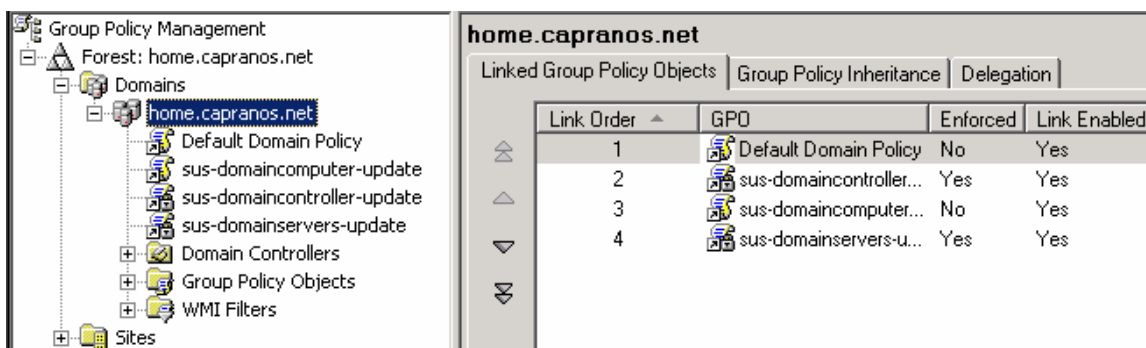
The use of Windows Active directory and Group Policy will be discussed in the next section.

Active Directory Integration--Using Group Policy Objects With WUAU Policy

Microsoft's SUS by itself is not very functional, and while it does bring the benefits of Windows Update website to the corporate network, to receive the full benefits of a centrally administrated service, computers have to be configured to download all new updates from the SUS server. For computers to receive updates automatically, the use of Windows Update Automatic Update (WUAU) policy and Active Directory using group policy are required.

The WUAU policy needs to be placed on all Windows computers that will use the SUS service. For this to work, an administrator would have to go to each computer on the network and manually configure this option. However, if Microsoft's Active directory is in use, a new group policy with the WUAU policy can be created to point Windows computers to the SUS server.

Group policy is a powerful tool in Active Directory that allows administrators a great deal of centralized control over how best to update Windows computers and servers on the network. The creation of Group Policies allows administrators to have more control over what groups of computers download new updates. Group policies can be used to create different time periods for when Windows computers download their updates. An example being: downloading updates based on departments or office locations to help reduce traffic on the network. The home.capranos.net domain has three Group policies put in place for the different types of computers placed on the network, which are Domain Computers, Domain Controllers, and Domain Servers. An example of such Group Policies is show below.



(Screen capture of SUS-Group policies for home.capranos.net)

By having Group Policies put in place for the different groups of computers on the network, this allows a greater control over when the updates will be downloaded and applied. On the next page there is an example of the Group Policy with WUAUI policy that was created for Domain Computers group.

Microsoft's System Update Services

Administrative Templates		hide
Windows Components/Windows Update		hide
Policy	Setting	
Configure Automatic Updates	Enabled	
Configure automatic updating:	4 - Auto download and schedule the install	
The following settings are only required and applicable if 4 is selected.		
Scheduled install day:	0 - Every day	
Scheduled install time:	12:00	
Policy	Setting	
No auto-restart for scheduled Automatic Updates installations	Enabled	
Reschedule Automatic Updates scheduled installations	Enabled	
Wait after system startup(minutes):	10	
Policy	Setting	
Specify intranet Microsoft update service location	Enabled	
Set the intranet update service for detecting updates:	http://backup.home.capranos.net	
Set the intranet statistics server:	http://backup.home.capranos.net	

(Screen capture of SUS-Group policies for home.capranos.net)

The above Group Policy specifies the Windows Update Automatic Update settings for the Domain computers group that are on the home.capranos.net domain. The above policy shows that Automatic Updates have been enabled for the domain computers organizational unit (non-domain controllers), and that the computers will automatically download and install updates which are scheduled to be installed daily at 12:00 pm. To prevent users from losing valuable work, no auto-restart was enabled; updates will be applied after the next restart of the computer. Lastly, the above Group Policy specifies the intranet SUS server where the Windows computers will download their updates, and where the statistics are stored.

Using group policies ensures that Windows computers will receive updates which will help centralize the update system reducing the amount of time needed for administrators to go to each computer and configure automatic updates. By setting Group policies for different departments, this helps to reduce the possibility of extreme loads on the network. However, administrators must ensure updates are being applied; SUS does offer basic monitoring and logging tools, but these tools don't offer a great level of information and in some instances any information at all. Several third party companies are offering products that will keep up to date statistics of what updates have applied to Windows computers from SUS. In the next major revision from Microsoft, Windows Update Service (SUS v2.0) will offer a more comprehensive set of monitoring tools than the current version of SUS.

What Software Update Services Can and Cannot Do

Microsoft's Software Update Services is an installable version of the Windows Update website that is centrally located on the corporate network. It synchronizes with Microsoft's Update Servers to download and host available patches, updates and security fixes for the Windows XP, 2000 and 2003 operating systems. The Software Update Service is a useful tool to help administrators approve updates that will be sent out to Windows computers on the network. The use of Active Directory and Group Policy helps to ensure Windows computers are receiving the necessary updates. However, SUS is not a complete update service and is incapable of completing other tasks, which will be discussed in the following paragraphs.

Microsoft's Software Updates Service is very good at what it does, but it does have a few limitations. SUS is only capable of patching at the operating system level (including Windows Explorer and Internet Information Services), but is incapable of patching other Windows applications such as Microsoft Exchange, SQL and Office products. SUS is limited to patching Windows XP, 2000 and 2003 operating systems; and previous versions such as Windows NT 4, 95 and 98 are simply not supported. Additionally, SUS can not deploy custom patches for third party applications or software.

A feature that is severely lacking in Microsoft's Software Update Services is the inability to scan Windows computers that are attached to the network; such an inability prevents administrators from knowing which computers need to be updated.

It is worth mentioning that SUS also has limitations with Windows 2000; SUS is only supported under the following conditions:

- Windows 2000 (Professional, Server, and Advance Server) with service pack 2.

Once service pack 2 has been applied, the Windows 2000 computers will be able to receive updates from the SUS server.

Recommended System Requirements

In this section, a brief overview of the system requirements for SUS will be discussed. If SUS is to be used in a production environment, an available server with the minimum requirements needs to be made available; and depending on the operating system, additional licenses may be needed. Microsoft's Software Update Service requires basic hardware support and the recommendations are as follows:

- Pentium III 700 MHz or higher processor
- 512 MB of Ram
- 6 Gigabytes of available disk space

The above are the recommended system requirements; however, SUS can be installed on a system with lower capabilities. An example would be the SUS server on the home.capranos.net domain. The SUS server is a Dual Pentium Pro 200 MHz system with 1024 MB of Ram. Increases in system requirements only become more important as the number of Windows computers increase. Shown below is a depiction of increasing system performance as the number of Windows computers increases.

- 1 to 20 Computers, Pentium II 400 w/ 512 MB Ram
- 21 to 50 Computers, Pentium III 500 w/ 512 MB Ram
- 51 to 100 Computers, Pentium III 700 w/ 512 MB Ram
- 101 to 500 Computers, Pentium IV 1000 or higher w/ 512 MB Ram
- 500+ Computers, Additional SUS servers.

As the number of Windows computers using SUS increases, the requirements for the system also increases. The recommended number of Windows computers that SUS can support is 500. If additional support is required, the deployment of additional SUS servers will be necessary to support additional Windows computers. Another consideration to be made is office location. When there is more than one office on the corporate network, having additional SUS servers at each office will reduce the load on a single server, and will help reduce the amount of traffic traversing a WAN link.

Finally; the recommended operating system for SUS is Windows 2000 or 2003. However, it can be configured for use on a Windows XP Professional system with IIS 6.0 installed.

Future of Microsoft's SUS

SUS is a small component of the System Management Software currently offered by Microsoft. SUS is being offered to help time strapped administrators centralize their Windows Update schema on the corporate network. SUS is a free download from Microsoft, and will hopefully remain so; however, SUS like any product does have a limited shelf life. Microsoft is currently working on Windows Update Service (WUS), which is a vast improvement over SUS, offering a better management interface and increased logging of updated Windows computers. Windows Update Services is currently in the Beta Phase of development; so the finished product will not be released for quite some time.

For the time being, SUS is a good short term solution for ensuring a centralized control over what updates are being applied to Windows computers. Many of the techniques that were used in the deployment of SUS will be identical to that of Windows Update Service (WUS).

Conclusion

Microsoft's Software Update Services is an installable version of the Windows Update website. SUS allows administrators with the use of Active directory, Group Policy and the WUAU policy, centralized control over how Windows Computers will download / install patches and security updates. By synchronizing with Microsoft's Update Servers, new updates are downloaded by a few SUS servers and hosted locally; this helps to reduce the amount of traffic on a WAN link. By having centralized control over how, when, and where Windows computers will receive their updates, this reduces the amount of time administrators will have to spend ensuring Windows are being updated. SUS is still lacking some features: to be fully effective as a complete Windows update and installation service, monitoring and logging features are required. Currently, only third party software or hobbyist add-ons are available for this role. An example being, GFI LAN guard Network Security Scanner.

In the next major release of Software Update Services (SUS v2.0 or Windows Update Services) monitoring and logging features will be incorporated to give administrators yet another level of centralized control, and will continue to reduce the amount of time spent on ensuring Windows computers are being updated. This will help to reduce the number of vulnerabilities on a corporate network and will increase the up time of Windows computers.

References

Microsoft's Software Update Services, MCSE World by Daniel Petri
<http://www.petri.co.il/sus.htm>

Microsoft's System Update Services

Patch Management in the Windows World, SUSserver.com, by Scott Korman
<http://www.susserver.com/Articles/Win-PatchManagement.asp>

Automatic Update Settings via Group Policies, SUSserver.com, by Scott Korman
<http://www.susserver.com/Articles/AU-AutoUpdateGroupPolicy.asp>

Installing SUS – Basic Installation, SUSserver.com, by Scott Korman
<http://www.susserver.com/Articles/SUS-InstallingSUS-Basic.asp>

Software Update Services Overview White Paper, Microsoft.com,
<http://www.microsoft.com/windowsserversystem/sus/susoverview.mspx>

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