Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

Perhaps everyone has suffered from computer problems that resulted in virus, hacker data loss and system vulnerabilities. So, since 1998 Microsoft has released a method to update patches when use Windows operating system via www.windowsupdate.co website

Perhaps everyone has suffered from computer problems that resulted in virus, hacker data loss and system vulnerabilities. So, since 1998 Microsoft has released a method to update patches when use Windows operating system through the websitewww.windowsupdate.com.When using Win XP or Win 2K SP3 or later, we have a new feature called A *utomatic updates* that can automatically connect to the windows update site to download the system patch files.

Picture 1 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

Automatic Updates program automatically updates the patch

However, in a distributed environment, the single update of patches for the system is often not highly effective due to many reasons such as sugar. transmission, difficult to manage due to the carelessness of users. So in the role of IT Supervisor or Network Administrator, we probably want a more efficient method of processing.And fortunately, SUS can solve that problem for us, with SUS we can manage the update of system patches for users through one or more susserver intermediary servers.And the A *utomatic updates* program on users' computers will be configured to connect to the server to download updates instead of from the Microsoft website. This will help us manage the process of updating the system more effectively with mechanisms such as scheduling updates to clients or specifying files to be installed. based on *domain* policy.

In this article, I will present the method of installing, configuring sus server and setting up domain policies on a real model of a customer company with more than 50 users to be able to manage and deploy counter. Update the system more effectively.

The TestLab model needs the following machines:

Step 1: Install and Configure Software Update Services

Software Update Services (SUS) is a completely free, downloadable product from *http://www.microsft.com/downloads* and proceed to install on susserver.mcsesecurity.com.The installation process is relatively simple, we only need to specify the location to store the necessary files of the program and follow some instructions given as shown below.

Picture 2 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

After the installation process is complete, the next step is to log into the admin websitehttp://susserver.mcsesecurity.com conduct data synchronization with Microsoft server update and perform some necessary configuration operations.

Picture 3 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

Administration website of Software Update Service server

Click *Synchronize* to download the fixes from Microsoft servers, because the volume of updates is quite large, it takes a long time for the data synchronization process. Therefore, in order to limit bandwidth usage, we should set a schedule for this process to take place outside the working time by selecting *Synchronizer Scheduler* and setting the following parameters:

Picture 4 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

When the synchronization process finishes, depending on your system, you can select the necessary hotfixes to let the clients update through the A *utomatic updates* utility by selecting *Approve updates* and checking the files to patch for the machines. Online:

Picture 5 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

List of patches and options

So we have installed and configured the sus server. Next, we just need to configure the auomatic update program on the clients connected to this machine to download the patches to install again.If the client computers on the network do not have the Automatic updates utility, they can be downloaded from the Microsoft download website and distributed to the member machines through Group Policy or instructing the user to install them from a shared folder. Check the Cntrol Panel again when the installation is complete to ensure that Automatic Updates is available on your system.

Picture 6 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

Step 2: Configure Group Policy on the domain controller

We manage the patch update process for the client through Group Policy on the domain admin machine through the following actions:

1. Select Start -> Program-> Admnistrati Tools-> Active Directory User and Computer

2. Click the right mouse on the domain and select Properties, then select Group Policy, select Default Domain Security Policy and click Edit to open the domain's policy editor and select Add / Remove Templates as shown below:

Picture 7 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

3. Select the ADM (administrative template) named wuad.adm and click Open

Picture 8 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

4. Then we edit the policy by clicking Automatic Update in the right pane of the *WUAU-ADM template and selecting Auto download and scheduler the install* and determining the date and time for the client to download the system update files. About as shown below:

Picture 9 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

5. Next, click on the Specific intranet Microsoft Update server location and select enable then enter the name of the sus server and select OK:

Picture 10 of Update bug fixes for distributed environments via SYSTEM UPDATE SERVICES (SUS)

So we have completed the SUS server system and created the necessary policies so that the agents can download patches from the grave. specific servers in the domain system.Following this, we run hGPupdate.exe from the Run command and ask users to restart the system when possible.

Note: For computers in a Workgroup environment we can still deploy this model by changing the local policy of each machine.

To ensure the safety of the system when a problem occurs, we should make backup of necessary data of the *sus server* .To backup your content, the website of administration and iis metabase, you can see more about this issue at microsoft site or contact the email address at the end of the post to get more information.

However, some patches may cause older applications on the system to become unstable, so for systems that are critical we should thoroughly check patch files on test machines and refer to Carefully review the production information about their side effects.And in order to know which computers on the system have not updated in time for this vulnerability, we should use automatic scanning programs provided by Micorosoft. Offer like Hfnetchk or MBSA, these are The program can be downloaded for free through the Microsoft download website.

References - You can download books, demo video files and programs at the following address:

http://www.security365.org/downloads/books

http://www.security365.org/downloads/demo

http://www.security365.org/downloads/software/

Nguyen Tran Duy Vinh, NetManager - MCP

An Security Solution Company

www.security365.org

consultant@security365.org