RealTime
CONSULTING SERVICES

Windows NT 4.0 and Windows 2000 Service Pack and Hotfix Deployment Best Practices

Standards and Guidelines for Management and Deployment

Prepared by: Al Guevara
Rev. 04/02/03

I. Purpose

The purpose of this document is to establish general standards and guidelines, or Best Practices, in the identification, deployment, and management of Windows NT and Windows 2000 service packs and hotfixes in an organization's enterprise.

II. Identifying new patches

The best way to become aware of fixes is to proactively search for them before they are needed. You can always go to the Microsoft web sites for Service Packs, Hotfixes, Security, and Knowledge base items. However the information presented can be daunting even when you know what you're looking for.

a. Subscribe to the Microsoft Security Bulletin service:
   1. Go to http://www.microsoft.com/technet/security/default.asp
   2. Then click on "Want to receive future security bulletins automatically?" and follow the procedure to subscribe. You should get several confirmations from Microsoft Security and start receiving the bulletins.

b. Subscribe to the NTBugtraq mailing list:
   1. Go to http://www.ntbugtraq.com
      This is useful when searching for a hotfix for a particular problem.

Correlate any pertinent bulletins with information received from 3rd party Service Pack and Patch Management tools, if being used.

III. Evaluation

You must first determine whether a patch is needed before deciding to install it. As a rule, Microsoft recommends not loading a hotfix unless you are experiencing the particular problem that it is supposed to fix. Every hotfix is not meant to be installed as it is released. The exception to this would be a fix that addresses a serious security vulnerability. Depending on the severity or potential impact, you would not wait for the problem to occur before deciding to apply the fix. Pay attention to the type of server the hotfix addresses – for example, all file servers, IIS servers only, or e-mail servers. Not all fixes are applicable or needed for every type of server. Also, weigh the potential impact with the problem it fixes.

IV. Testing

Patches should always be tested before deploying. Although Microsoft almost always recommends loading their patches, you will notice that the technical notes pertaining to the patches also recommend that the patch or hotfix be thoroughly tested in a lab environment, before loading in a production environment. The reason for this is that Microsoft does not perform regression testing on their hotfixes, meaning they are not extensively tested or tested with every type of software, driver, or hardware. The patch needs to be tested against the hardware and configurations specific to your environment. While you may not be able to test on all possible hardware, software and configurations, what you are looking for are incompatibility and stability problems. The purpose is not just to test the patch or update, but to test the implementation process as well, whether it be via manual method, package distribution, or service pack management tool.

Next, testing should be done on a limited-production basis – that is, deploy to least significant servers or to a small number of servers representative of the various server types, such as file servers, web-servers, domain controllers, etc. During this time, planning should be in progress for deployment to the rest of the servers. A recovery or backout plan should also be developed in case of problems during or after the upgrades. You cannot and should not rely solely on updating the Emergency Repair Disks (ERDs). Appropriate backups and being prepared to rebuild a particular server should be part of a contingency plan.

V. Deployment

Deployment procedures should be the same as the processes tested. There are several ways to automate service pack and hotfix deployment, using Microsoft SMS, 3rd party tools, batch files or Microsoft Resource Kit tools (or a combination thereof).

VI. Managing and Tracking Service Pack and Hotfix Information

Unfortunately, there is no easy way to keep track of the hotfixes loaded on the servers (and even more difficult to track on workstations). Depending on the type of patch or hotfix loaded, not all methods will display accurate or meaningful information (i.e. the command Hotfix -1, run on the command line, does not seem to be consistent). Service Packs are a little easier. See the procedures below for methods in identifying service pack levels - particularly identifying whether SP6 or SP6a is loaded. Most of the native NT tools and even most 3rd party tools cannot differentiate between SP6 and SP6a. As long as SP6 no longer exists on a given network, this will not be a major issue. (However, there are still organizations running on version NT 4.0 SP6).

For large enterprise environments, using a 3rd party service pack and patch management tool is the easiest and most effective way to keep tack of service packs and hotfixes. Service Pack Manager 2000 is an example, which we have used for a large fortune 100 client, for service pack and approved hotfix deployments.

a. **Service Pack Manager** (currently SPM 2000)

This utility basically saves time, resources, and energy in managing and deploying service packs and hotfixes. Service Pack Manager queries the computers on the network and displays information about what Operating System and what service packs and hotfixes are loaded on each NT or Win2K server or workstation. It checks it against information on it's database that you can update by performing a scheduled LiveUpdate It also remotely installs service packs and hotfixes, and reboots the machine accordingly. It includes an embedded browser that points you to Microsoft's web site pertaining to a particular service pack or hotfix, including the pertinent Knowledge Base article and source of download.

The User Interface is easy to maneuver and all the basic procedures are covered in the Help tab. Some other helpful features are **NetGroup**, where you can define groups of networked computers, using aliases; **User-defined Hotfixes**, that allow for SPM installation of hotfixes not available in the SPM database; and the **Profiler** feature, that allows you to test computers against pre-defined or user-defined groups of hotfixes (this is useful once you know what service packs and hotfixes to look for).

NT 4.0 Service Pack 6a System Requirements

- 60 MB of storage space for x86 and Alpha.
  (120 MB if selecting uninstall feature.)

- No previous Service Pack needed.

- Windows NT Workstation 4.0, Windows NT Server 4.0 or Windows NT Server 4.0 Enterprise Edition installed.
  (Does not update Windows NT Server 4.0 Terminal Server, which has its own Service Pack.)

Checking whether NT 4.0 Service Pack 6a is installed

Winver.exe – run this utility at the command line to correctly report whether the service pack is SP6 or SP6a.

Registry key – check **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Hotfix\Q246009\Installed** = 1 registry key. The value 1 indicates SP6a is installed.

Note: For machines with SP6 or SP6a loaded, checking via Microsoft NT Diagnostics (Winmsd on the command line) is not enough as it will always show as SP6. For Compaq machines, Compaq Insight Manager will also display SP6 whether it's SP6 or SP6a. Unless you are using a service pack management program, the two methods highlighted above are the most accurate ways to verify whether SP6 or SP6a is installed.

Service Pack and Hotfix Deployment

Prerequisites – for the person(s) applying service packs and hotfixes.

Preparation

1. Read the Readme.txt file for the particular service pack or hotfix to be installed for issues, requirements, and procedures. Note specific procedures on installation sequences for various server applications (IIS, Exchange Server, SQL Server, etc.).

2. Update the Emergency Repair Disk.

3. If this is a file server or other server containing important data, make sure the server has been backed up.

4. Disable services not required for start-up, including third party services (especially pcAnywhere, virus scanners, and scheduling programs). Ideally, remote control software, such as pcAnywhere, should be uninstalled prior to applying the service pack. Microsoft application services should be set to manual and stopped (i.e. Exchange services, SQL services).

5. Ideally, the machine should be rebooted with no errors prior to loading a service pack.

6. Check the Event Log for errors *before* and *after* applying the patch.

7. You should choose Create the Uninstall Folder option when installing a service pack.

Prior to implementation, a WinNT / Win2K Service Pack and Hotfix Listing should have been created, containing the organizations current standards, and approved service packs and patches for the various type platforms. Consult this document prior to loading patches on servers in the production enterprise.