



Standards and Practices

S&P Article ID: SAP-005

Title: Best Practices for Server Configuration

Description: Procedures to provide quality, consistency, and reliability during the server build process.

Revision / Date: 1.1 / 2007-01-29

Status: Final

Author: Glenn Barnas

Client Approval:

Server Configuration Best Practices

Server Design Considerations

Use of Standard Locations

This document assumes that servers will have at least 3 drives. The O/S will be installed to C:, the pagefile will be defined on D:, and the application components will be installed to E:. The CD-ROM drive will be configured as R:. The assignments used are examples for this document and may be different in your environment. The key is to configure these assignments consistently on all servers.

- Consistency of server configurations is critical in an environment where many people support the same system, and even more so when different departments support specific components of these servers. Communication of these standards between departments is essential.
- System Administration tools, used primarily by but not limited to the IT team members should reside in C:\local\bin. This folder should be used for any single command-line tool used to aid in system administration, as well as a common location for all scripts and batch files. Additional components related to S/A tasks should also be placed in the \local directory structure. This includes *perl* (where appropriate) in \local\bin\perl.
- Applications – anything not directly related to the Operating System but supported by the IT team – should be placed in a subfolder of Program Files. Applications that are integrated with the O/S or are critical to the operation of the system (such as IIS or backup utilities) should be installed on the C: drive. All others should be installed on the E: (application) drive.
- All IS logs (event logs, performance logs, etc) should be maintained within the \Local folder structure. When long-term archiving is needed for audit purposes, a separate, dedicated folder should be employed, allowing special security and backup procedures to be employed.
- Applications should be placed in a folder on E:, such as \APPS. With the advent of mountable file systems in Windows 2000, this would provide a seamless and transparent method to migrate customer applications to larger disks or SAN storage. It also permits a clean isolation of applications on shared systems.
- The use of a dedicated paging file drive is strongly recommended. Where supported, this should be a separate spindle or volume. A separate logical partition should be created from within the O/S if a physical volume is unavailable. The physical size of this volume should be 12-15% larger than the desired page file size to prevent capacity warnings from the O/S or other monitoring tools.

Top-Down vs. Bottom-Up Build Approach

- A top-down build process using “smart-start” type methods proceeds by installing all optional components, leaving the system overloaded with components that must then be removed. Uninstalling a component may not necessarily remove the associated data folders and related log files. This results in a system that may have more components loaded and running than required. It also presents issues when uninstalling components that aren’t needed. Often, you can install “Component A” without installing “Component B”, but when both are installed together, uninstalling “Component B” may affect (or require the un-installation of) “Component A”.
- A better approach is to manually install the server O/S, selecting only the components that are universally required. Any specialized component can then be added during the server customization. This minimizes the number of running services and eliminates the overhead and complexity of running services and components that aren’t required in a specific configuration.

System Management & Administration Concerns

Windows Resource Kit

- The resource kit consists of numerous *unsupported* tools used to aid in system administration. Many are simply examples of tools that can be developed in a Windows environment. Because they are not supported by Microsoft, they are not checked for vulnerabilities, or patched on a regular basis. Because of this, the entire resource kit should *never* be installed on a production server.
- The tools of the resource kit should be reviewed, and an appropriate subset installed. Only tools regularly used for diagnosing problems or managing installed applications should be deployed. Deployment should be to the S/A tools folder (local\bin). Some tools that are rarely used or could be used to compromise security can be maintained on a central file server, making them available to authorized users when needed. A collection of common tools will be listed in an appendix to this document.

Inappropriate Services or Drivers

- Incorrect or inappropriate drivers and services can cause problems that are difficult to diagnose, as well as mask other problems. The installation process should be carefully reviewed to insure that only current and necessary components are installed.

Interactive Server Applications

- The use of interactive applications as server services is strongly discouraged! These configurations result in environments that are less secure and very fragile – susceptible to service interruption due to account lockout or user logoff.

- The use of alternative products that run as system services should be investigated. When these are not available, the application should be configured as a service using the Windows SrvAny component.

Programs Installed In Root Folder

- Programs installed to the root create a clutter of folders, resulting in additional management overhead and a potential reduction of system performance. It also increases the possibility of security vulnerabilities, as installation processes may alter permissions on their folder.
- Commercial applications (such as ColdFusion) should always be rooted to E:\ drives if they must be rooted at all. Installing them to E:\Program Files or E:\Apps is a much better alternative when possible.
- Separate folders should be used for each application, and on shared servers, there should be isolation – both physical and permission – between each application component.

\Local\Bin Directory Structure

- This path contains tools and scripts that are used by the IT team for System Administration. Not having these tools can limit the diagnostic ability of the persons supporting the system.
- The complete set of tools should be installed on every server during the build process. All tools should be re-installed with possibly updated versions during annual maintenance.
- The install process creates three System environment arguments – S_CONFIG, S_BIN, and S_LIB, which point to the root folder, bin subfolder, and lib subfolder respectively. These variables allow scripts and other tools to easily locate these folders without hard-coding the applications.

Inappropriate Applications Installed on Server

- Application could be installed on servers, either as part of the O/S or an integral component such as IE. These components are end-user applications, and serve no purpose on an application server, and can expose significant security risks. Examples of these applications include:
 - Microsoft Front Page – web page editor, end user tool
 - Script Debugger – can be exploited by hackers
 - Microsoft Front Page Extensions – add-on for web servers, should not be installed unless specifically required by the application.
 - Outlook Express – SMTP email client component
 - NetMeeting – end user tool
 - NNTP (when installing IIS components). Install only when required by an application.

- These applications should be removed from existing servers; Server images should be built without these components; Installation packages should be developed so that add-on software automatically excludes these products and components from the install process.
- Once these tools are removed from servers, updates & patches for these components should not be applied to production servers, as the patch will often install a full update, installing it where it did not exist.

Log Files Replicated in System Image (Sysprep) – and –

Empty Folders in Directory Structure from Uninstalled Applications

- Special attention should be given to the image creation process, especially clearing event logs and removing any application logs. The presence of these logs can mislead initial diagnostic efforts.

Unused folders should also be removed. Empty folders unnecessarily add to the diagnostic overhead when searching the system for elusive problems. The directories serve no valid purpose for the application or management of the server.

System Volume Information Directory

- This directory is used by the system for file system security and recovery purposes. After a normal installation, this folder is accessible only by the System account. Changing the permissions on the root of a drive can affect these permissions. Care should be exercised when changing drive root permissions to exclude this folder.

System Paging File placed on Dedicated Drive

- The system paging file should not be placed on the NT System disk to obtain best performance, per Microsoft recommendations.
- Most SAN vendors recommend against placing paging files on SAN storage.
- Tests have shown that utilizing a separate physical partition (from the RAID controller) or physical drive (non-RAID configurations) for the paging subsystem significantly contributes to the overall performance. When this is implemented, the recommended target drive letter should be “D:” to keep it well isolated from production drive letters.

Rapid Deployment Considerations

To accommodate the rapid deployment of similar systems, imaging technology can be employed. With Windows systems and Microsoft Sysprep, images of the initial system load can be quickly installed on a raw server, allowing a “mini-install” to take place. This completes the basic configuration, registers installed hardware, and can even install select applications.

If extreme care is not given to the creation of the host machine, imaging technology can deploy a corrupt or incompatible image just as quickly as a finely tuned one. Some guidelines specific to creation of the host image include:

- Use one image for each brand and model. While Windows mini install can accommodate changes in plug-and-play hardware, subtle changes in the integrated peripherals, including the CPU revision and the supporting chipset can develop into difficult to isolate, intermittent problems later in the deployment.
- Create a minimal host image. Only the required O/S components and a minimal set of service packs or hotfixes. Remember, it's easier to add software than remove it! With the use of automated installation tools (such as SWDIST), service packs, packages of hotfixes, and even complete applications can be installed and configured with a minimum of user interaction.
- The host server configuration should be serialized and carefully documented. The version number should be placed into the registry to allow software to determine that a system was built via cloning, and which image type and version was used.