University Information Technology Services

Windows Server Security

Best Practices

Initial Document

Created by: 2009 Windows Server Security Best Practices Committee

Document Creation Date: August 21, 2009

Revision

Revised by: 2017 Windows Server Security Best Practices Committee

Revision Date: April 28, 2017

Version Number: 3.0.5

Acknowledgments

The final release document is a collaborative work between the following committee members:

Freddie Lewis

Khushbu Desai

Theodore McDonald

Tanya Sootes

Usage

The ever changing nature of information technology prevents this document from being entirely inclusive but should serve as a general guideline. This document is not intended to supersede or replace policy. Please feel free to query the Windows Server Team (winserv@kennesaw.edu) or the Systems Administrator Group (SysAdmin@list.kennesaw.edu) for additional guidance.

Table of Contents

1. Infrastructure Best Practices

Every server should have a designated functional purpose along with primary and secondary administrators, who will take responsibility for and correct any problems it may have.

All servers, before (or immediately after) going live and on a regularly scheduled basis, must submit to a security scan by the Information Security Office to ensure it meets all criteria supplied by the ISO.

1.1. Physical Security

Servers should always be located in a secure, locked area ideally equipped with card-key access by authorized personnel only. Should an intruder gain access to a Windows server or its console, serious damage or data theft could occur. For example, Servers are vulnerable to "Live CD" boots and mirrored switch hubs.

As appropriate, for servers involved in a mission critical process, it is suggested the physical area of the servers and consoles be under constant camera surveillance.

Keep a record of physical access. The access log generated by the server room card-key system should be kept indefinitely, or as required by local or state regulation.

1.2. Power

Servers should always have Uninterrupted Power Supply(UPS, for example). This is for the protection of the server hardware (offering some isolation from power surges, sags, and spikes). It also protects information on server hard drives by allowing the server to be gracefully powered down in an extended power outage. How long the redundant power system must support servers during a power failure is a function of the criticality of the servers. In non-critical, academic settings, a few minutes of redundant power may be all that is needed to smooth over a brief outage. However, for mission-critical servers, it may be necessary to provide the capability of 24 by 7 redundant power.

1.3. Fire Control

Servers should not be placed in an area covered by a fire suppression sprinkler system. In such circumstances, even a minor fire can result in complete loss of servers and storage devices. Instead, the server should be located in server rooms which employ a non-conductive (FM200 or similar) fire suppression system.

1.4. Climate Control

Server hardware is most reliable when it is operated in a cool environment. If the server room is too warm, seek assistance from campus physical plant operations to determine how the room can be better cooled. There should be a physical climate monitoring system in place.

2. Redundant and Failover Configuration

2.1. Redundant Servers

Whenever possible, failover servers or appropriate redundancies should be in place to prevent downtime in the case of a disaster.

2.2. Clustering and Failover

If the operation of a server is critical, consider server clustering and/ or server failover. Windows server software is capable of both. Ideally, for clustering server hardware should be as identical as possible.

2.3. Redundant Storage

Server hard drives are heavily used; therefore, it is important that some form of redundant storage be provided. It is not unusual to have a single hard drive failure in a file server. Various methods for protecting against such failures are available and should be employed. Servers support redundant storage in two ways.

2.3.1. RAID

Two or more drives can be installed in a Windows Server and various RAID configurations can be selected. RAID 0 uses a stripe set to write data across multiple drives. RAID 1 uses mirrored drives. RAID 5 uses a stripe set with parity (which allows a configuration to be rebuilt after the loss of a single drive). RAID 6 uses a stripe set with two parity drives. A common RAID configuration is RAID 1 for the operating system, RAID 5 with a hot spare for data, or if supported, RAID 6 for data on large drives (1TB and larger).

2.3.2. SAN

Optionally, redundant storage hardware can be purchased from many vendors. These redundant Storage Systems appear to a Windows server to be a single drive but provide continued operation in the event of a single drive failure. A storage area network is an alternative to using RAID drives. They provide a virtual storage environment made up of multiple hard drives, a piece of which is provided to particular servers for their use. Storage area networks typically employ one or more forms of redundant recovery to maximize uptime. Some SAN solutions also include automatic backup capabilities. Storage area networks are available from many server hardware vendors.

2.4. Virtualization

Virtualization offers another type of redundancy. Systems deployed in a virtual environment can be afforded protection from resource issues, such as power, memory, and storage. Hardware maintenance in the virtual environment usually does not require the guest server to be down as it can be moved to another host, thereby improving availability.

3. Security Best Practices

3.1. User Environment

Servers are for providing university services, not to be used as a workstation. Any interactive use of a server should be limited to the scope of the server's operational function. Activities like browsing the internet or reading email should be avoided. Further, applications designed for desktop use should not be installed on a server. Servers should have minimal installed applications while still allowing required functionality within the environment.

3.1.1. Server Account Control

Each individual should have a unique user id (netID) that can be referenced to a person's full name and contact information. The use of local accounts should be avoided. Accounts should have an expiration date. Accounts should be given only privileges that are needed. This applies to accounts for users, resources, applications, and service accounts. Also, the server should be audited at least on an annual basis to confirm which users are still authorized.

3.1.2. Administrator and Equivalents

The administrator account should be renamed and never used for day-to-day operations. The number of persons knowing the administrator login should be strictly limited. Use of Group Policy in Active Directory allows the creation of a new local administrator while at the same time disabling the Built-In Administrator account.

3.1.3. Delegating Control

Windows Active Directory allows control of Organizational Units to be delegated in lieu of using the administrator account or equivalents. This should be standard practice.

3.1.4. Password Policy

Passwords must be required for all accounts. Further, passwords should be required to be complex (a mix of letters, numbers, and special characters) or lengthy (as in pass- phrases.) Users should be required to change passwords at some regular interval. Passwords should always follow the specifications stated in current university policy.

3.2. File and Print Serving

3.2.1. Folder and NTFS Permissions

Be aware of the differences between folder share and NTFS permissions. It is normal practice to set share permission so EVERYONE has FULL CONTROL and then use NTFS permissions to regulate file level access.

3.2.2. Print Management

Be careful to set printer permissions to control access and take advantage of Group Policies that allow deployment of printers by user and computer (Windows Server 2008 and later.) They eliminate the need for scripts and the like to install printers on user PCs.

3.3. Remote Access

3.3.1. Terminal Services

If terminal services are provided, remote desktop access should be restricted to domain administrators and/or the primary and secondary administrators of that server.

3.3.2. Off-Campus Access

Off-campus access should be restricted to VPN-authenticated users.

3.4. OS Configuration and Maintenance

3.4.1. Security Measures

3.4.1.1. Disable Unused Services

Windows Server has many processes it uses to provide a wide array of services to users. Not every server uses or needs every service to be either installed or running. Any services that can be stopped, disabled, or removed without adversely affecting the performance of the system should be so configured.

For Windows 2008 and later, Microsoft has taken the approach of role-based services only being added to the server as needed. Services not needed for the roles being used are not installed. There is also a Server Core installation option which further removes many unnecessary components or services.

3.4.1.2. Updates

Currently, Microsoft releases updates to its operating systems on a monthly basis. However, updates of a more urgent nature may be released off-schedule due to importance. Because of the constant security threats against servers, it is important to apply updates from Microsoft as quickly as possible after they are released. It is recommended, however, that patches released on "Patch Tuesday" be applied to test a system (or a group of test systems as appropriate to the environment) and monitored for a minimum of 5 days to verify application functionality and determine any adverse performance impact. During this time, it is also wise to research any known issues associated with patches and ensure countermeasures are in place. Patches can then, in most cases, be safely deployed to remaining systems according to a schedule coordinated with stakeholders.

3.4.1.3. Service Packs

Periodically, Microsoft bundles all previous updates and corrections for Windows Server into a service pack. Service packs, when installed, simply replace files that have been corrected by Microsoft. It is recommended to apply a service pack to a test system first while waiting a period of time before deploying the service pack to production systems. Microsoft has, in the past, released defective service packs. Once a service pack has been released, a minimum of 30 days should be allowed to confirm the service pack's functionality. Testing of the service pack in a particular environment is highly encouraged along with internet research for any known issues associated with the service pack.

3.4.1.4. Server Applications

Patching or updating server applications is also important. The same testing and research associated with operating system service packs should also be performed with server application updates or patches. Additionally, the associated application administrators and customers should perform this process as much as possible.

3.4.2. Audit Practices

Servers have a powerful auditing feature built-in. It is usually disabled by default but can be easily enabled. Typically, server managers would want the auditing system to capture logins, attempted logins, logouts, administrative activities, and perhaps attempts to access or delete critical system files. Auditing should be limited to gathering just the information that is needed, as it does require CPU and disk time for auditing to gather information. Log Management software should be used, if possible, for ease of managing and analyzing information. Auditing in most cases can be enabled by group policy, so any new servers added into the associated OU will have it automatically enabled and turned on.

3.4.2.1. Log Retention

Servers keep multiple logs and, by default, may not be set to reuse log file entries. It is a good practice to expand the size of the allowed log file and to set it to reuse space as needed. This allows logging to continue uninterrupted. How far back log entries go will depend on the size of the log file and how quickly log data accumulates. If the server environment is critical, it may be appropriate to ensure that the log file size is sufficient to store the required logging information as dictated by current university policy. Doing so would allow going back to any previous log file entries via the event viewer (as might be required for an audit or legal issue). If a system log server is employed, the local log storage time may be reduced.

3.4.2.2. Auditing

Preserve, review, and analyze logs as appropriate for the environment. The ISO group can provide guidance regarding best practices to protect the university.

4. Attack Footprint

4.1. Security Software

Servers are vulnerable to many forms of attack. Implementation and standardization of security methods should be developed to allow early and rapid deployment on servers. It is important that Windows servers be equipped with at least the following protective software:

4.1.1 Antivirus and Antispyware

Users may unknowingly place virus infected files on the server, which may be shared among other users, thus infecting additional systems. Every Windows server should have some form of virus scanner that is kept current with the latest virus definitions.

While it is unlikely that an end user will cause spyware to infect a Windows server, it is possible that a server administrator, accessing the Internet from the console, might unknowingly cause spyware software to infect a server. For that reason, it is reasonable to install anti-spyware software directly on a server and to make sure that it stays up to date.

It is strongly encouraged that you use the approved antivirus and antispyware application. Please contact iso@kennesaw.edu for more information on the approved security software.

4.2 Network Traffic

Kennesaw State University employs a campus firewall that protects the campus environment from most Internet threats. However, the Campus firewall does nothing to protect servers from threats generated on campus. For that reason, it is reasonable to employ some form of a software firewall on a Windows server. At minimum ports not required to be open for the server to function properly should be blocked by a host firewall.

4.2.1. Windows Firewall

Windows has a Firewall that is included by default with any current server OS. Best Practice is to have only necessary ports open and, if possible, restrict access to those ports to necessary IP addresses. The firewall can also be configured to restrict access to/from applications and protocols.

4.2.2. Software Host Firewall

There are a number of third-party software vendor firewalls available. The Windows Team and/or the ISO can offer guidance in selecting one if desired, but does not offer Support for any of these at this time.

4.2.3. Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) can be implemented as another layer of security, along with a firewall, protecting communication over IP on your server.

5. Change Control

System administrators should maintain a log, written or electronic, of all changes to the operating environment, to include hardware, system security software, operating system, and applications. Additionally, a baseline of services, open ports, mount points should be documented to support future changes. Prior to any changes being implemented on a production system, the system administrator should receive approval from the change management team. The team should be comprised of stakeholders and IT professionals.

6. Disaster Recovery Practices

6.1. Backups

It is very important that servers be backed up on a regular basis. Depending on the use of the server, it may be adequate to back up the server once per week. A backup of a more critical environment may be needed daily, and possibly continuously.

The backup program provided with Windows is capable of backing up to virtually any writable media, which can include network drives provided by a server in another physical location. This program is also capable of scheduling backups which can ensure backups occur on a regular interval. Should a more sophisticated backup program be required, there are several excellent choices available in the marketplace.

6.2. Offsite Backup Storage

It is very important that one backup set is taken off site on a regular basis. This is to prevent a total loss should the physical facility be lost in a fire or other disaster. Offsite backup storage should adhere to current university policy.

6.3. Test Backup Restores

It is critical that a backup set periodically be fully restored to a test system. This is to demonstrate that the backups are functioning as they should, and can be restored when necessary. It is suggested that a backup set restore be tested once per quarter, but once a month might be appropriate in more critical environments.

7. References and Resources

This document is intended to serve as a brief introduction to activities and guidelines that should be followed by all managers of servers. This guide is intended to be very practical and thus is a little shy on details. Plenty of documents can be found on the Internet, which describes Windows Server best practices in detail.

The reader should also be aware that Microsoft offers an excellent resource for Windows Server managers called TechNet found at http://technet.microsoft.com/en-us/ and Microsoft

Events found at http://msevents.microsoft.com/

Microsoft also makes available in excellent series of documents related to Windows Server Best Practices. Those documents cover basic configuration, operations, and security. Certainly, some of the most important documents are the Windows Server

Windows Server 2008 Security Guide, found at:

http://www.microsoft.com/downloads/details.aspx?FamilyID=fb8b981f-227c-4af6-a44b-b115696a80ac&displaylang=en

Also with the release of Windows Server 2008 R2 rather than providing a copy to every baseline operating system, Microsoft provides Security Compliance Manager 2 (SCM 2). SCM 2 is a free tool from the Microsoft Solution Accelerator. More Information and download information can be found at:

http://technet.microsoft.com/en-us/library/gg236605.aspx

Microsoft also provides an excellent tool called the Baseline Security Analyzer for analyzing the security configuration of any Windows workstation or server. Through its use, the user can learn what weaknesses exist in the setup of the Windows Server operating system being analyzed. The Baseline Security Analyzer also provides excellent recommendations based on any weaknesses that it finds. The Baseline Security Analyzer can be located at:

http://www.microsoft.com/technet/security/tools/mbsahome.mspx