Windows Server Security Best Practices

Revised
05/13/2021
Version 2.0.1

Initial Document

Created by: 2009 Windows Server Security Best Practices Committee

Document Creation Date: August 21, 2009

Revision

Revised by: 2019 Windows Server Security Best Practices Committee

Revision Date: May 13, 2021

Version Number: 2.0.1

Acknowledgments

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

- Casey Darrow
- Davide Gaetano
- Chase Elliot

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. Security Best Practices

1.1. 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.

1.1.1. 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 follow the password expiration policy. 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.

1.1.2. 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.

1.1.3. Delegating Control

Windows Active Directory allows control of Organizational Units to be delegated to a user or group in lieu of using a shared administration account. This should be standard practice.

1.1.4. Password Policy

OCS insert KSU policy here or reference the document.

1.2. File and Print Serving

1.2.1. 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. For newer systems we will be moving away from this practice and use the same

groups used by the NTFS permissions with the share permissions. These permissions should be given to a group when possible. Using role based access control group delegate access such as READ, WRITE, or ADMIN permissions. SMB2.0 or higher should be used due to SMB 1.0 vulnerabilities.

1.2.2. 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. They eliminate the need for scripts and the like to install printers on user PCs.

1.3. Remote Access

1.3.1. Remote Desktop

Remote desktop access should be restricted to domain administrators and/or the primary and secondary administrators of that server. Enhanced security such as network level authentication should be enforced for connecting users and computers. This service should be blocked by a firewall and only allowed through a trusted encrypted service such as a VPN.

1.3.2. Off-Campus Access

Off-campus access should be restricted to VPN-authenticated users. Access to servers through the VPN for either application administration or server management will be done through a role based VPN.

1.4. OS Configuration and Maintenance

1.4.1. Security Measures

1.4.1.1. 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.

1.4.1.2. Updates

Currently, Microsoft releases updates to its operating systems on a monthly basis via patches and rollups. However, updates of a more urgent nature may be released off-schedule due to the importance and/or severity of the issue. 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 systems 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.

1.4.1.3. Service Packs

Certain server grade software like Microsoft SQL Server, periodically issue service packs containing security and bug fixes. Administrators of this level of software should take into consideration the schedule and impact these service packs have on their systems.

1.4.1.4. 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 and maintain this process as much as possible.

1.4.2. 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. Logs such as system, security, and application logs should be monitored. Any logs that produce trackable or important information should also be monitored and alerted upon if needed.

1.4.2.1. 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 or redirect entries to a logging server. 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. Logs should be kept upon an agreed upon time per the standard set by your business unit. This standard should factor in any business needs for keeping logs for a minimum amount of time. It is recommended to keep at least 30 days or longer.

1.4.2.2. Auditing

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

2. Attack Footprint

2.1. 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:

2.1.1 Antimalware

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 scanner that is kept current with the latest definitions and scanning engine.

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

It is strongly encouraged that you use the approved antimalware application. Please contact ocs@kennesaw.edu for more information on the approved security software.

2.2 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-based firewall.

2.2.1. 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. Newly created systems should have it enabled, while existing systems should move towards having it enabled.

2.2.2. 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. This firewall standard can be used as an alternative to the traditional Windows firewall but it is recommended to use the Windows Firewall controlled by group policy.

3. 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.

4. Disaster Recovery Practices

4.1. 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 daily. A backup of a more critical environment may need additional protections than standard backups. The backup program provided with Windows can back 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 that the processes occur on a regular interval. Should a more sophisticated backup program be required, there are several excellent choices available in the marketplace.

4.2. 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 standard and any BOR standard.

4.3. 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 on a routine basis at least once per month.

5. 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

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