Windows Server Security Best Practices

Revised
05/13/2021

Version 2.0.1

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

E-0

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 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 syste6 (n)1.1 In11 Tf 0.002 Tc -0.002 Tw 0.283 0 Td [(S)4.1 (er)d Td [((er)c

appropriate to ensure that the log file size is sufficient to store the required logging information

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 servers. This firewall standard can be used as an alternative to the traditional Windows firewall bu-4 (y)c5 (to)2 (th)-4 (y)c5 (to)2 (th)-4 (y)c5 (to)2

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