Windows Server Configuration Guidelines

The following guidelines and best practices can be used to secure Microsoft Windows servers on the NAU network and to protect the data housed on them. The use of the word "server" indicates either a physical or virtual server where files or services are being used. In some instances the guidelines and configurations described may not apply to a given department or college. Some departments and colleges may have certain regulations to comply with, such as the Payment Card Industry, PCI, regulations.

It is recommended that each department maintain documentation about the servers used in their areas, the roles each server fulfills, the firewall configurations, user access, and other strategies put in place.

If your department or college will handle credit card data NAU Policy requires you contact ITS to help you meet the PCI-DSS regulations. Please contact Information Technology Services, ITS, at 523-1511 to receive assistance meeting the regulations.

The ITS Department offers hosted services that may help you avoid managing your own servers. To see if ITS can help with cost effective solutions for server or other needs, please review the following information and contact 523-1511 for more details.
http://www.nau.edu/ITS/Services/ServerHosting/

ITS also has a license for Qualys Vulnerability Management scanning. Contact us if you would like to learn more and potentially configure scans of your servers to help identify potential vulnerabilities.

Do You Really Need a Server?

ITS offers many hosted solutions to the rest of campus. Listed below are some data technologies that ITS offers as a service.

Web Hosting – Ektron CMS, Apache, Tomcat, IIS
Application Server Technologies – ASP, JSP, PHP, CGI
Database Technologies – MySQL, Oracle SQL
File Servers – Windows Share Drives (Samba), SFTP

Table of Contents

Physical Security

Servers should be secured in locked areas with restricted access.

Installation, Activation & Configuration of Windows

Installation can be done via install media or based on an image/template from a previously secured server. There is more than one domain that a server can be joined to and they each offer different options for the system administrator. ITS recommends joining one of the NAU domains (students or nau) after the Windows Server OS installation has completed. This allows for settings to be applied automatically via Group Policy Objects, GPO, either at the top-level domain or within a departmental Organizational Unit, OU.

- The nau domain, for example, has top-level default GPOs that will automatically configure many of the settings described in this document. This helps a system administrator manage settings centrally with the default ITS configurations.
- The students domain offers the option for system administrators to manage their own OU and create, apply, configure, and modify GPOs that fit the needs of the department.
    - The nau domain also offers this same option.
- This document will refer at times to the default GPOs available in the nau domain. The GPO configuration settings in an ITS-managed OU can be explained in depth.
- Please contact the ITS Department at 523-1511 to learn more about the two domains, the different options available, and which will work best to fulfill the needs of the department.

Manually set the IP addresses (static assignment) for each server. NAU has a public IP range and a private IP range available. Any server that does not need to access off-campus networks and does not need to be accessed from off-campus networks can use the private network. Windows servers can get their security updates from the local WSUS server in either case. To learn more about the IP address options available please contact ITS.

Activation

When joining the nau domain the activation of Windows should occur automatically via KMS activation and should be confirmed. Note that this could take a couple of restarts, following updates for example.

Confirm that the network time and time zone were set automatically when joining the domain and change if needed.

Updates & Antivirus

The server should have the latest OS and application updates applied. If necessary, Windows Updates should be installed first thing. By joining an ITS-managed OU in the nau domain, a GPO will enable and configure automatic updates as well as install antivirus software.

- A well-defined update and antivirus strategy should be established. If you need assistance configuring a server to use the WSUS server contact ITS.

- Routine maintenance, including patching and updating, should be regularly scheduled and documented.
- Antivirus software should be installed, updated and activated. NAU has a campus license for Sophos Endpoint Security; therefore it is the recommended antivirus product.
- Consider disabling the automatic clean-up of malware on mission critical application servers. It is best to configure the antivirus software to isolate/quarantine the infection for manual evaluation as false positives can cause downtime or data loss. Automatic cleanup could be more appropriate on a file server or terminal server, where non-administrators are allowed access to shared resources.
- Evaluate the need for on-access scanning in antivirus software. On-Access scanning will be initiated with each read and/or write to the disk - this can create additional overhead and unnecessary processing/resource drain on busy servers.
- Configure a regularly scheduled full system scan.
- In some scenarios it will be best practice to configure email alerts or notifications in the antivirus software. In the case of an unattended server, for example, no one will be logged in to see the default desktop alerts.

Windows Firewall and Services

The firewall should be enabled and configured with the most restrictive settings possible. By joining an ITS-managed OU in the nau domain, a GPO will enable and configure windows firewall settings.

The following practices are a small set of a Windows firewall and services strategy. Contact ITS for more details about the full configurations in this GPO.

- Configure the firewall with the most restrictive settings possible.
- Configure the firewall to allow only the IP range(s) expected.
- Unused services should not be allowed to start as 'automatic' and ports should be evaluated.
- Remove all unnecessary services, features or applications from the server. These may differ based on the role the server will fill.
    - Some examples of services to disable are Telnet and FTP.
    - Disable web browsing on servers unless running a terminal server.

User Accounts and Passwords

Default accounts and default or weak passwords should be disabled, renamed, or modified.

The following should be part of an account and password strategy.

- Disable or rename the Administrator account.
- Disable all generic Guest accounts and consider renaming them.
- Disable all default passwords, or at a minimum change to very strong passwords.
- Restrict the use of blank passwords.
- Do not allow auto-login.
- Enable screen saver, screen-locking.

- Disable the setting that reads as “Interactive logon: Do not require CTRL+ALT+DEL.”
    - In other words, retain the default to require CTRL+ALT+DEL setting.
- For more information about strong passwords and password management best practices:
    - http://www.nau.edu/its/learn/PasswordChangeProcess/

Remote Desktop and Access Control

The file system should have a well-documented access control strategy allowing for only authenticated user access. By joining an ITS-managed OU in the nau domain, a GPO will enable and configure remote desktop. Contact ITS for more details about the full configurations in this GPO and others.

The following should be part of an access control and remote desktop strategy:

- Remote access should be disabled or restricted to specific IP addresses by default, such as NAU VPN address space. Contact ITS to obtain the VPN address information.
- Directories, files, and shares should be evaluated for permissions, including close analysis that the Everyone group not be given access to shares with sensitive/secure data.
- Administrative shares, such as C$, should be disabled or audited for access.
- No open or non-authenticated file sharing should be allowed.
- All service accounts should be evaluated and granted access to the minimum levels needed.

Auditing, Backup & Recovery

By joining an ITS-managed OU in the nau domain, a GPO will enable and configure some auditing and event log management settings. Contact ITS for more details about the full configurations in this GPO and others.

The following should be part of an auditing and event log management strategy:

- A strategy should be established for regularly reviewing audit logs, either manually or programmatically. This should include system logs and service logs. The types of services to monitor will differ based on the role each server is provisioned for.
- Audit account logon events, account management, directory service access, policy change, system events.
- Auditing of privileged accounts should be enabled, specifically on failure.
- Auditing of administrative share access, if used, should be enabled.
- Disaster recovery planning for each server should be documented and include details about the back-up methods, recovery and restoration of the system and applications as well as data.
- At least one backup should be stored in a different location as the server itself.

Server Roles

When provisioning a Windows Server for a specific role there are additional items to consider for further securing the server. When planning and provisioning your server layout, designate one primary purpose per server. Whenever possible, designate one server as the database server, one server as the web server, and one server as the file server. An example of best practices and guidelines for the Web Server

Role is included here. Some in depth information can be found using the link provided below for these more common server roles.
http://technet.microsoft.com/en-us/library/hh831669.aspx

Web Server Role

Follow the best practices and guidelines for securing the server listed above first, and then:

- Install only the IIS modules that are needed in order to reduce the attack surface.
- Periodically review the IIS modules and handlers in order to remove those not being used.
- Keep an antivirus program updated. NAU has a campus license for Sophos Endpoint Security; therefore it is recommended.
- Isolate or separate web applications into different sites and application pools.
- Isolate or separate ASP.NET temp folders by site and give access to the identity appropriate for the site.
- Plan for anonymous/windows authentication and disable the ability for anonymous writing.
    - Configuring Anonymous with another authorization type can lead to problems in the order of precedence in the modules being run. For example, the "second" listed type may not run at all.
    - For writing, or uploading, use an authentication method other than anonymous.
- Enable request filtering rules in order to help block potentially harmful HTTP requests from reaching the server.
- Limit the permissions being given to non-administrators.
- Establish and perform regularly scheduled backups.

File Transfers

Follow the best practices and guidelines for securing the server listed above first, and then consider the role your server will play in file transfer – will it be sending only, receiving only, or both? Using WinSCP for the sending of files to another server is a secure method of transferring files out. If establishing a receiving server for file transfers be sure to use SFTP and strong user/password combinations, firewall settings, and all other OS best practices.

Test or learn more about your Web Server's default SSL/TLS protocol configuration, cipher suite configuration, and certificate status using the following free, online, resources. In particular, 2014 saw several vulnerabilities to SSL and current best practices include disabling SSL, enabling TLS, where impacts to services will not be experienced.

- https://www.ssllabs.com/ssltest/
    - ***Be sure to check the "Do not show the results on the boards" box***
- https://sslanalyzer.comodoca.com/

General server side SSL/TLS best configuration practices can be found here:

- https://wiki.mozilla.org/Security/Server_Side_TLS

Disposal

Media destruction takes several forms, including physical destruction or electronic destruction. Physical destruction of media can take several forms, such as drilling holes in the physical drive. Electronic destruction needs to follow certain guidelines, and ITS suggests the standard DoD and NIST guidelines
for 3-pass wiping of a drive. More details about the NIST Special Publication 800-88 can be seen here: http://www.nist.org/nist_plugins/content/content.php?content.52.

One such tool for performing the multi-pass drive wipe is found here:
http://www.dban.org/

PCI Compliance

Some departments and colleges may have certain regulations to comply with, such as the Payment Card Industry, PCI. If your department or college will handle credit card data please contact Information Technology Services, ITS, at 523-1511 to discuss the requirements.

Additional Resources

Information Technology Services at NAU

- Server Hosting at ITS
  - http://www.nau.edu/ITS/Services/ServerHosting/
- Password Management Tips
  - http://www.nau.edu/its/learn/PasswordChangeProcess/

Microsoft TechNet Windows 2008 R2
http://technet.microsoft.com/en-US/windowsserver/bb310558

Microsoft TechNet Windows 2012
http://technet.microsoft.com/en-us/windowsserver/hh534429

Microsoft Server Security and Protection Overview, provides new feature descriptions in 2012:
http://technet.microsoft.com/en-US/library/hh831778

Microsoft Baseline Security Analyzer Tool, to help identify missing updates and common security misconfigurations when setting up a new server:
http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=7558

Microsoft Security Compliance Analyzer provides a full set of documents into one tool:
http://www.microsoft.com/en-us/download/details.aspx?displayLang=en&id=16776