Server Protocols

Contents:

- Definitions
- Baseline Configurations
  - Hardware
  - Software
  - Management
  - Environment
- Purchasing Server Class Systems or Applications

UNCW is experiencing a significant increase in servers located in both the central computing facility and in offices and departments across campus. These servers are being used for production and non-production disk space, serving applications and to meet the research needs of departments. As the number of server systems increases, so does the concern for the management and security of these systems. To address this issue the university needs a university-wide server protocol standard that will address the purchasing, implementation, management and security for these systems.

The Information Technology Systems Division is concerned that there are servers that are not being maintained in a manner that protects the content of the server, the campus network and users, as well as networks and users outside UNCW. Data or applications that are critical to the university should utilize ITSD services. These services and their host systems are up-to-date, backed up and are included in a disaster recovery plan. Data or applications that are critical to a department should either utilize ITSD services or be maintained on hosts equivalent to those directly supported by ITSD. In several cases where non-ITSD servers or systems are being utilized, security and backup protocols are not being effectively addressed.

When servers are not updated with the latest security patches, they are susceptible to intrusion from attacks. Servers are more vulnerable to attacks due to the increased number of services they run (IIS, SMTP, FTP, etc.) than standard desktop systems. Once one of these servers is compromised it may attack other machines inside and outside of our network, creating complex security issues and increasing possible liability issues for the university.

Of even greater concern is the fact that some server owners have modified their servers to deny ITSD the ability to scan for compliance and audit issues.
To reduce the potential for an interruption of services, reduce the liability exposure of the university and to maintain a level of server standards and compliance, the following server baseline configurations have been established. Failure to follow these protocols could result in the removal of a server from the network.

**Definitions:**

*Production Server*
A computer which provides some service and/or information to other computers connected to it via a network. The loss of use of a production server would disrupt the unit or university’s ability to function.

*Server (network) Operating System*
An operating system designed to host servers and/or services to be accessed by client and/or remote systems. These include, but are not limited to: Windows Server 2003, Windows Server 2008, Linux, Solaris, Netware, AIX, UNIX, OSX, and other network operating systems.

*Baseline configuration*
Minimal systems requirements for hardware, software, and system administration.

**Baseline configurations**

*Hardware Baseline Configuration*
- The computer must be server class hardware sized properly (CPU, Memory, Disk Space) for the applications and all hardware must be at the current version of firmware. Desktop systems should not be used.
- Disk space should be separated with the OS in one container and applications and data in others. It is recommended that all partitions be protected against single drive failure using RAID 1 or higher.
- Backup hardware and/or software must be implemented on all systems and must be able to backup the entire system(s) and data. This can be tape, RW-CD, RW-DVD, or any other removal media.
- Systems must have current active hardware maintenance and support contracts.

*Software Baseline Configuration*
- The server (network) operating system must be the latest version available with all security and system stability patches installed.
- All installed software must be properly licensed.
- Where possible, virus protection software must be installed and maintained.
- System, security, and application logging must be at a level that will assist in resolving issues.
- It is strongly recommended that maintenance and support contracts be maintained on applications.
Management Baseline Configuration

- The unit will name a responsible party and alternate for each system.
- ITSD must have administrator access to the system for compliancy scans. Systems that do not allow this access are subject to be removed from the UNCW domain and the network ten days after a second notification.
- Disaster Recovery and Business Continuity Plan must be in place that addresses backup times, types, rotation and offsite media storage.
- System and security logs will be monitored for events.
- The patch management procedure must be documented and implemented.
- Server management and non affiliate/vendor access will be administered in accordance with the ITSD Policies.
- Best practices guidelines provided by the vendor should be followed.

Environment Baseline Configuration

- The server is to be located in a secure location with limited controlled access.
- The location will have environmental controls that keep the temperature and humidity at a level specified by the hardware manufactures.
- The server must be on UPS power.

Purchasing Server Class Systems or Applications

To assist departments with compliance issues the purchases of server hardware and (network) operating systems will be routed through and signed off by ITSD OSA. The purchases of enterprise applications will be routed through and signed off by ITSD Technology Needs Assessment and Consulting. Approvals are contingent on:

- Departmental need and justification for a service that is not or cannot be provided by ITSD.
- Mutual agreement to a Service Level Agreement.
- Compliance with the baseline configurations stated above.

Revision History

February 19, 2010 - Updated ITSD department names to reflect ITSD reorganization. Updated OS system names.