Standards for Connecting Servers to the University Network

ITS Standards

Introduction

The purpose of this document is to identify a set of standards that server systems must meet in order to operate on the University at Albany's network. This document is not intended to impart all knowledge required to operate or secure a server, but rather to identify topics and procedures that System Administrators should be familiar with and prepared to address.

What is a Server?

Any machine (virtual or physical) which has services open to other computers is considered a server. This includes embedded devices such as networked copiers, printers, industrial control systems, desktops, laptops, tablets, or other devices that offer services to network systems. Each server must be actively administered by a system administrator who should ensure that the server complies with the University at Albany Server Standards outlined below. Please note that any services that are publicly accessible from the Internet or accessible from the UAlbany campus intranet create potential security problems, hence the need to actively manage them.

Virtual Systems

All the standards apply with equal force regardless of whether the server is a virtual or physical system. Additionally, there are two requirements unique to virtual machines that system administrators must comply with. System administrators who decide to employ virtualization should acquaint themselves with the key areas related to risk management which are identified in the section entitled: Preparing a Virtual Server for the UAlbany Network.

UAlbany Network Server Standards

In order to run a server system on the UAlbany Network the following standards must be met:

1. The server must be accounted for in NetReg with ownership and contact information clearly indicated.
2. The server must be managed by at least one system administrator (See note 1).
3. The server should be running a current operating system as well as a current version of the service (See note 2).
4. Patches should be evaluated and applied in a timely fashion by the system administrator (See note 3).
5. The server should be configured in a secure manner (See note 4).
6. If the server holds Category 1 data, it must meet all applicable regulatory requirements (See note 5).
7. Only properly licensed software should be run on the server.
8. The server or service must not interfere with any UAlbany Enterprise services (e.g., DHCP, DNS).
9. The network services provided by the server must be configured to be accessible from the minimum set of systems and networks as determined by the server's business or academic requirements.
10. The system administrator must have a method to continuously acquire, assess, and respond to information that identifies vulnerabilities to facilitate remediation, and thereby minimize the window of opportunity for attackers. Note: The University provides such a service in the form of Tenable's Security Center. Please see the AskIT wiki article for more information.
11. Virtual Systems: Where data of different levels of sensitivity are commingled within a virtual environment, however that environment is defined, controls required to assure the confidentiality, availability, and integrity of the most sensitive data should be applied.
12. Virtual Systems: Access to the hypervisor environment should be isolated from regular production access and be strictly limited in terms of network ports, source systems, and personnel, employing a range of safeguards to prevent unauthorized intrusion.

Notes:

1. A system administrator in this context is defined as an individual, or team, who is responsible for the setup, maintenance and ongoing operation of the server.
2. The term "current" is used to define an Operating System and/or Service which is maintained by either a vendor or community to ensure that identified vulnerabilities or performance issues are dealt with in a timely manner.
3. Patches refer to any updates available for the Operating System and Software installed on the server system.
4. "Secure manner" refers to the procedures outlined in the "Preparing a Server for the UAlbany Network" section.
5. "Category 1 data" refers to any data which falls under regulatory requirements such as, but not limited to: HIPAA, FERPA, GLBA, and Personally Identifiable Information as defined by the NYS Information Security Breach & Notification Law. In addition, it encompasses any data that the University declares especially sensitive. For a full definition of the University's Data Classification Standard, see here.

Preparing a Server for the UAlbany Network
Procedures for running a server on the UAlbany Network. Additional details for each numbered item are available below.

1.1 Verify that your computing needs are not already met by existing UAlbany ITS or departmental servers.
1.2 Assign a system administrator team to setup, maintain, and monitor the machine.
1.3 Take appropriate precautions during the installation of a server and/or software.
1.4 Environmental and physical controls.
1.5 Install a current version of the OS and service(s).
1.6 Perform and validate backups and archives.
1.7 Turn on logging.
1.8 Disable default accounts and sample scripts; change any default passwords.
1.9 Only activate/operate needed services.
1.10 Restrict network access.
1.11 Setup only secure methods of authentication.
1.12 Configure administrator level accounts to be compliant with the university's Privileged Access Standard
1.13 Employ file integrity checks on system and configuration files.
1.14 Designate your server as a server system in NetReg.

Preparing a Virtual Server for the Albany Network

The following key areas relating to risk management should be taken into account when considering virtualization.

1.16 Virtualization software, such as hypervisors, represents a new layer of privileged software that will be attacked and therefore must be protected.
1.17 The potential loss of separation of duties for administrative tasks can lead to a breakdown of the defense in-depth approach. Role definition and separation of duties must be properly planned for in a virtual environment.
1.18 Patching, signature updates, and protection from tampering for production, as well as offline, VM and VM appliance images needs to be accounted for.
1.19 Virtualization can result in limited visibility into the host operating system and virtual network to find vulnerabilities and assess system configurations (e.g., file integrity checking, log inspection).
1.20 Likewise, virtualization can limit the view of inter-VM traffic for inspection by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
1.21 Security tools for virtual environments may not provide the same level of visibility and protection as they do for physical systems.
1.22 Business processes and policies should be applied when defining the organizational roles and responsibilities for processes and authorities within the virtualized environment.

Maintaining Services & Security on a UAlbany Server

Staying Connected and Ongoing Maintenance

2.1 Review service logs and backup logs regularly.
2.2 Periodically review running services and evaluate the continued need for those services/server(s).
2.3 Apply vendor/community provided updates regularly for both the OS and applications.
2.4 Regularly monitor and maintain all user accounts.
2.5 Maintain current registration information in NetReg.

Preparing a Server for the UAlbany Network: Details

1.1 Verify that your computing needs are not already met by UAlbany ITS or departmental servers.

Before you decide to undertake the task of installing, configuring, securing, and operating your own server on the UAlbany network, check that the services you require are not already being provided by Information Technology Services, or your own department's server systems. Your department's Technology Coordinator should be able to assist you in this.

1.2 Assign an administrator to the machine

Someone must be assigned to properly manage a server. Their responsibilities include keeping up to date with security issues and assuring the system's availability and reliability. Failure to properly carry out these responsibilities can result in lost service or a compromised system.

1.3 Take appropriate precautions during the installation of a server and/or software

We suggest that when setting up a new server you do so in a protected environment. This will allow you to download patches but it does not expose you to would-be hackers looking for your machine. Consider the use of a hardware firewall or installation of the server system and/or software and any required patches "off-line."

1.4 Environmental and Physical controls

When configuring a server system, it is important to consider the location of the server. The University at Albany has determined that servers should be located in the UAlbany Data Center unless a review by ITS Staff finds it is not possible to house the server in the UAlbany Data Center. The reason for this is that a server must have a location that will not only provide the appropriate power and cooling but provide a means for physically securing the server. In order to ensure the security of the data contained on the server, the machine itself must be secured. By housing servers in the UAlbany Data Center potential attackers will not have physical access which would allow them to simply walk away with your sensitive data. Generally, any machines which are in public areas should not be considered physically secure and should not be utilized as servers.

1.5 Install a current version of the OS and service(s)
If you are using an operating system or software which is no longer supported by a vendor or community effort, your servers may have several known and un-patched exploits and vulnerabilities.

If you absolutely need to run an old OS or software for some reason, virtualization, a private IP address, or a hardware firewall may be the best solution.

If a server is found to be exploited due to the use of an old OS or Software, the machine will not be allowed back onto the network until the OS and/or software is upgraded and/or the device is logically or physically isolated from the public network.

1.6 Perform and check backups and archives

No server system can be complete without backups. Not only are they good as a matter of practice but they can be vital in restoring the security and data integrity of a damaged or compromised server system. In the event that a machine is compromised you may have no choice but to revert to previously backed up copies of various data. As such it is important that each server have a backup schedule and that backups are tested on a regular basis to ensure the process is successful.

1.7 Turn on logging

In order to effectively monitor the security and integrity of your server, you should enable reasonable logging of events. Logging of server activity, including but not limited to Internet traffic, can help establish normal or suspicious patterns of activity. Additionally, once you have a baseline for "normal" events, you can identify anomalies which can indicate performance issues or unauthorized access.

1.8 Disable default accounts and sample scripts

Any account you have on your system is a potential doorway for intruders to gain access. Default accounts give attackers the advantage of knowing which doorknobs to rattle. Disabling default accounts is an important security precaution. Most modern operating systems do not install default exploitable accounts, however, several software packages do. Database products install several default accounts and passwords which must be changed before the server is exposed to the Internet. Also note that software may contain sample scripts or test configurations which are not designed for production use. These should be disabled and/or removed before the server’s configuration is complete.

1.9 Only activate/operate needed services

Every service you run on a server is another administrative layer that carries its own potential vulnerabilities and security issues. If you are not using a running service, you are unnecessarily exposing the machine and increasing your workload. The last thing you want is to have your server hacked because of a service you weren't even using. Keep an eye out for default services which may be running on a newly installed system, or come with newly installed software. Often these services need to be configured so that only the appropriate personnel are using them.

1.10 Restrict network access

Consider the use of a firewall or host-based filtering software. A vendor provided firewall provides you with an extra level of security by allowing you to restrict access to those ports you open. Similarly, host-based filtering software such as ipfilter and tcpwrappers can assist in ensuring that only those machines that have legitimate reasons for connecting to the server will be given access.

Services should be configured so that they are accessible only from users, systems, and networks with a justifiable business or academic need for access. Services should be accessible from the Internet only if there is a documented requirement to do so. Otherwise the service should be configured to be accessible only from the UAlbany intranet and if access from off-campus is needed, use of the University's VPN solution is required.

1.11 Setup only secure methods of authentication and authorization

Currently, authentication comes in many flavors: something you know (e.g., password), something you have (e.g., RSA token), or something you are (e.g., fingerprint). Systems that employ more than one of these use multi-factor authentication. No matter which one you choose, make sure that you use it securely. Even secure authentication needs to be maintained or it ceases to be effective.

**Authentication**

- **Centralized authentication**
  - Binding to ITS’ managed LDAP directory services such as Active Directory (preferred method) or LDAP 389 for authentication allows users to login to a system using their University provided NetID and password.

- **Passwords**
  - The most common type of authentication, passwords offer the advantages of being free and easy to set up. However, in order for passwords to be secure they should follow these guidelines:
    - They should not be used over insecure protocols (e.g., telnet, FTP, HTTP). If you use passwords over these protocols, they are not secure. The passwords are sent in plain text over the network to reach their destination. Use secure protocols for password authentication such as ssh.
    - You should use complex passwords or long passphrases for all accounts. Simple passwords are vulnerable to guessing and dictionary attacks.
    - You should never use the same password or a password with minor variations (such as: password1, password2, etc.) on multiple accounts. This is especially true if you have received a privileged account for administrative tasks in addition to your personal account.
    - Keep your password confidential. The only value your password has is its confidentiality; once that is compromised, it is worthless.
Passwords must be unique, i.e., not previously or currently used in connection with other services or systems. This is especially true if you have received a privileged account for administrative tasks. Minor variations of existing passwords are not considered unique. You can test whether a password has been previously used by visiting https://haveibeenpwned.com/Passwords.

**ID-Card/SmartCard**
Cards which contain integrated circuits capable of authentication can be purchased from various security companies. As with biometric identification, the cost and use of such systems should be weighted against the need for security.

**Biometric Identification**
Various biometric identification systems are available which use a variety of methods to authenticate an individual.

**Authorization**

**Group Access**

- If you are connecting to an ITS Directory Server for authentication, authorization should be implemented using Directory Server groups. This will help ensure resource access is audited by ITS Staff, which is crucial to maintaining the security of University data, systems and applications.

1.12 **Configure Administrative Accounts**
Configure administrator level accounts to be compliant with the university’s Privileged Access Standard

1.13 **File integrity checks**
File-integrity checking software should be used on those files that control user, system, and application settings. Depending on the nature of the attack, file integrity checks may be the only way to detect the intrusion. Examples of such software include but are not limited to: Tripwire - http://www.tripwire.com/

1.14 **Designate your server as a server in Net-Reg**
Designating your system as a server allows us to prioritize notification if a problem occurs, minimizing the potential exposure of data or disruption of services.

Maintaining Services & Security on a UAlbany Server: Details

2.1 **Review service and backup logs regularly**
Unless system and backup logs are reviewed regularly they have no value as a detective control. Making sure that your backups are completed successfully is vital to assuring that you have the ability to restore any critical data.

2.2 **Periodically review running services and evaluate the need for those services/server**
It is vital that you periodically evaluate the actual need for running services and/or servers. If a service is no longer being used, stop it. It will be one less thing to maintain and one less point of attack on your machine. If a server is no longer required, shut it down. It is natural to neglect a server that no one is actively utilizing. Unfortunately, this makes your server a prime target for hackers seeking to exploit un-patched and unattended machines.

2.3 **Apply vendor/community provided updates regularly**
Installing a current OS is great, but if you do not keep up with vendor/community provided updates, you run the risk of performance and security issues. Most vendors and on-line-communities provide methods to install updates. Please see your vendor/community’s documentation for details.

2.4 **Regularly monitor and maintain all user accounts**
A crucial part of maintaining a server’s security is maintaining its accounts. Once an account is no longer needed it should be removed or disabled so that it does not provide an access point into the server. Additionally, it is also helpful to regularly audit users on the machine to see if there are accounts that were never authorized as this could be a sign of a security breach.

2.5 **Maintain current NetReg registration information**
NetReg requires an annual renewal of a system's UAlbany network registration. Keeping the information up-to-date ensures that we have the right contact listed for the server you are maintaining. It also ensures that you will be contacted as soon as possible if we detect a possible problem.

**Additional Information:**
Below you will find links to various sites containing information about secure configurations, scanning tools, patches and updates for various operating systems and software. Some patches and updates may only be available if you have a support contract.
<table>
<thead>
<tr>
<th>Microsoft Products</th>
<th><a href="http://www.microsoft.com/security">http://www.microsoft.com/security</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows OS and Software</td>
<td></td>
</tr>
<tr>
<td>UNIX Operating Systems</td>
<td></td>
</tr>
<tr>
<td>Mac OS X</td>
<td><a href="http://www.apple.com/swupdates">http://www.apple.com/swupdates</a></td>
</tr>
<tr>
<td>FreeBSD</td>
<td><a href="http://www.freebsd.org/security/">http://www.freebsd.org/security/</a></td>
</tr>
<tr>
<td>NetBSD</td>
<td><a href="http://netbsd.org/Security/">http://netbsd.org/Security/</a></td>
</tr>
<tr>
<td>OpenBSD</td>
<td><a href="http://openbsd.com/security.html">http://openbsd.com/security.html</a></td>
</tr>
<tr>
<td>Linux Operating Systems</td>
<td></td>
</tr>
<tr>
<td>CentOS</td>
<td><a href="https://www.centos.org/">https://www.centos.org/</a></td>
</tr>
<tr>
<td>Debian</td>
<td><a href="https://www.debian.org/security/">https://www.debian.org/security/</a></td>
</tr>
<tr>
<td>Red Hat</td>
<td><a href="http://www.redhat.com/security">http://www.redhat.com/security</a></td>
</tr>
<tr>
<td>SuSE</td>
<td><a href="http://www.suse.com/security">http://www.suse.com/security</a></td>
</tr>
<tr>
<td>Ubuntu</td>
<td><a href="http://www.ubuntu.com/usn">http://www.ubuntu.com/usn</a></td>
</tr>
<tr>
<td>Security Standards and Information</td>
<td></td>
</tr>
<tr>
<td>The Center for Internet Security</td>
<td><a href="http://www.cisecurity.org/">http://www.cisecurity.org/</a></td>
</tr>
<tr>
<td>US-CERT</td>
<td><a href="http://www.us-cert.gov/">http://www.us-cert.gov/</a></td>
</tr>
<tr>
<td>SANS Institute</td>
<td><a href="http://www.sans.org/">http://www.sans.org/</a></td>
</tr>
</tbody>
</table>

Last Review: July 2015

Need more help? Contact the ITS Service Desk.