mac OS Server Security Best Practices

Revised – 05/13/2021

Version 1.1

Table of Contents

1. Initial Document

Created By: Michael Carroll (mcarro18@kennesaw.edu)

Document Creation Date: August 21, 2009

2. Revision

Revised By: 2020 macOS Server Security Best Practices Committee

Revision Date: 05/13/2021

Version Number: 1.1

3. Acknowledgements

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

- John Reeber

4. Usage

This document is intended to serve as a general guideline and should not be interpreted as policy. Furthermore, the ever-changing nature of information technology prevents this document from being entirely inclusive but should serve as a general baseline for server installation. Please feel free to query the System Administrators Group and ListServ for additional guidance.

5.3 Update Practices

5.3.1 Updates

It is very important that updates and patches be applied to servers in a timely manner. As Apple releases updates, they should be tested for compatibility with production software and systems and applied as quickly as possible.

5.4 Security Related Software

Servers are vulnerable to many forms of attack. It is important that a server be equipped with safeguards to protect the information resident on the system and the system itself.

5.4.1 Antivirus and Antispyware

Servers are vulnerable to a variety of malicious software through a number of attack vectors. Having the appropriate antivirus and antispyware tools running on a server and ensuring they remain up to date is extremely important to help combat this problem.

It is strongly encouraged that you use an antimalware client on all systems. Antimalware clients should receive updates daily and malware logs should alert an administrator in case of a found infection.

5.4.2 Firewall

Kennesaw State University employs a campus firewall that protects the campus environment from Internet threats. However, the campus firewall does nothing to protect servers from threats originating on campus. For that reason, it is reasonable to employ some form of a software firewall on a server. It is best to trust nothing on inbound and outbound traffic while only allowing the needed traffic through the firewall.

It is strongly encouraged that you use the built-in firewall, accessible in System Preferences → Security & Privacy --> Firewall. Please contact OCS@kennesaw.edu for more information.

5.5 Auditing Practices

5.5.1 Log Retention

Servers keep several logs and, by default, are set to reuse log file entries that are older than seven days. It's 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 your log entries go will depend on the size of the log file and how quickly you are accumulating log data. It is strongly encouraged that you keep at least 30 days of logs. It is important to arrange to rotate the logs in such a way that the size of the log files does not cause disk space shortages.

5.5.2 Auditing Practices

Most 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, log outs, 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. It is encouraged that administrators also use the Syslog solution provided by the UITS Office of Cybersecurity.

6. Mac Specific Security Best Practices

6.1 User Accounts

6.1.1 Securing Local Server Accounts

Unless administrator access is required, you should always log in as a non- administrator user. You should log out of the administrator account when you are not using the computer as an administrator.

Note: The guest account is disabled by default.. The guest account should remain disabled on all servers.

6.1.1.1 General Guidelines for Securing Accounts

Never create accounts that are shared by several users. Each user should have a personal standard account. User authorization can be managed through a rights dictionary; however, this is probably not necessary for server administration.

Each user needing administrator access should have an individual administrator account in addition to a standard account. Administrator users should only use their administrator accounts for administrative purposes.

When creating non-administrator accounts, you should restrict the accounts so that they can only use what is operationally required.

Accounts with administrator privileges should be used for login, and then the sudo command should be used to perform actions as root. Note: By default, sudo is enabled for all administrator users. You can disable root login or restrict the use of sudo command in the /etc/sudoers file. For more information, see the sudoers man pages.

You should create a group into which you put any user who needs administrator access. Then you can enable that group to have sudo access and the permissions will affect any user in that group.

To restrict sudo usage:

1. Edit the /etc/sudoers file as a user with sudo access using the visudo tool.
    a. $sudo visudo
2. Enter the account's password when prompted.
3. Remove the line that begins with %admin, and add the following entry for the administrative group:
    a. %*group* ALL=(ALL) ALL (Substitute the group's short name for the word *group*)

6.1.2 Disable the Root User

The root user is disabled by default and should not be enabled.
If the root user becomes enabled, you can disable the root account by using an administrative account and the dsenableroot command.

$ dsenableroot –d –u [user with admin privileges]

6.2 Password Policy

Passwords must be required for all accounts. Further, passwords should be required to be complex (a mix of letters, numbers, and special characters) or lengthy (as in pass- phrases.) Users should be required to change passwords at some regular interval. Passwords should always follow the specifications stated in current university policy.

6.3 System Security

6.3.1 Services Security

6.3.1.1 Configuring the Application Firewall

Follow these steps:

1. Choose System Preferences from the Apple menu
2. Click Security & Privacy
3. Click the Firewall tab
4. Choose Turn On Firewall
5. Click Firewall Options
6. You can click on the “+” button to add an application to this list. You can select an application and click the “-“ button to remove it. Control- clicking on the application name gives you the option to reveal the application’s location in Finder.

   Once you’ve added an application to the list, you can choose whether to allow or deny incoming connections for that application. You can even add command line application to this list.

   When you add an application to this list, macOS digitally signs the application (if it has not been signed already). If the application is later modified, you will be prompted to allow or deny incoming network connections to it. Most applications do not modify themselves, and this is a safety feature that notifies you of the change.

6.3.1.2 Security for Services Outside of Server Admin

Remote Access

Use SSH to secure Apple's Remote Desktop communications. This is the default behavior. SSH

- Use /etc/ssh_known_hosts to limit user's outgoing SSH connections. Create a secure tunnel when an insecure network may be involved.

6.3.2 Manage System Preferences

Desktop & Screen Saver

- Set Screen Saver to start after 20 minutes.

Mission Control

- Disable the Dashboard.

Security & Privacy

- Require password immediately to wake from sleep or screen saver.

iCloud

- Do not enable iCloud.

Network

- Turn off Wi-Fi.

Bluetooth

- Set Bluetooth to off.
- Also, disable allowing Bluetooth devices to wake computer.

Sharing

- File Sharing access should be restricted to required users/groups.
- Remote Login for SSH access should be limited to Administrators
- Remote Management should be limited to Administrators.
- Content Caching should be enabled on caching servers only.
- Other Sharing services should remain disabled.

Users & Groups Manager

- Do not enable the Automatic login.

- Select to display login window as Name and Password fields.
- Provide only the necessary administrative level for each user.

Date & Time

- Set NTP to the BlueCats: 10.54.38.5, 10.54.38.10

6.3.3 Configure Access Warnings

To create a login window access warning:

1. Open Terminal.
2. Change your login window access warning:
    a. $ sudo defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText "Warning Text" (Your logged-in account needs to be able to use sudo to perform a defaults write)
    b. Replace Warning Text with your access warning text.

SSH Warning Banner

1. Create a file call sshd_banner and add a message. Then, move it to `/etc/ssh/`
2. Edit `/etc/ssh/sshd_config`
3. Find the lines below and edit as follows:
    a. # no default banner path
    b. Banner /path/to/banner/file
4. Reload the sshd service
    a. sudo launchctl stop com.openssh.sshd
    b. sudo launchctl start com.openssh.sshd

7. References

- Mac OS Security Best Practices: https://help.apple.com/advancedserveradmin/mac/3.0/#apd83039B4A-6BD7-44B3-BCA5-C4CDB4542D57
- Apple Support: http://support.apple.com/
- Disable Root: https://support.apple.com/en-us/HT204012
- Application Firewall: https://support.apple.com/en-us/HT201642