Operating System Standard - Redhat Linux Configuration

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Industry Configuration Standards 3

1.5 Related Documents / References 3

2. Standard Statements 4

2.1 Redhat Configuration Baseline 4

3. Standard Compliance & Enforcement 15

3.1 Compliance Measures 15

3.2 Enforcement 15

4. Exception Process / Glossary 16

4.1 Exception Process 16

4.2 Glossary / Acronyms 16

5. Document Management 17

5.1 Document Revision Log 17

5.2 Document Ownership 17

5.3 Document Coordinator 17

5.4 Document Approvers 17

5.5 Distribution 17

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see XXXX-POL-ALL-001 - Information Security Policy Framework.

## Objective

The objective of this standard is to ensure the XXXXs business and technical requirements for Linux operating system are translated into a baseline that will allow administrators to easily configure new systems and compare existing systems to identify the difference between the current state and the starting point

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Industry Configuration Standards

* Centre for Internet Security (CIS): http://www.cisecurity.org/
* Security Technical Implementation Guides (STIGs): http://iase.disa.mil/stigs

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## Redhat Configuration Baseline

|  |  |  |
| --- | --- | --- |
| If this is a new system protect it from the network until the OS is hardened and patches are installed. |  | Required |
| Apply latest OS Patches |  | Required |
| Install and Configure SSH |  | Required |
| Install Zabbix | Install and Configure Zabbix on system | Required |
| Install and Run Bastille | Bastille is a system hardening tool for Red Hat and many other Unix and Linux systems. Bastille hardens the operating system based on the answers to a series of scripted questions. | Remove from list |
| **MINIMIZE XINETD NETWORK SERVICES** | **Description** | **Action** |
| Disable Standard Services | Xinetd has superseded inetd as the default network superserver. The stock configuration of both xinetd and inetd contain a number of standard services that are not necessary if the use of SSH as a secure login mechanism is present in the environment. | Recommended "Minimal" Installation | Other installation type: Required |
| Configure iptables | Configure iptables for minimum required access to ports. | Required |
| Only Enable telnet If Absolutely Necessary | Telnet uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and also that the session can be hijacked by outsiders to gain access to the remote system. | Required |
| Only Enable ftp If Absolutely Necessary | Like telnet, the FTP protocol is unencrypted, which means passwords and other data transmitted during the session can be captured by sniffing the network, and that the FTP session itself can be hijacked by an external attacker. | Required |
| Only Enable rlogin/rsh/rcp If Absolutely Necessary | The r-commands suffer from the same hijacking and sniffing issues as telnet and ftp, and in addition have a number of well-known weaknesses in their authentication scheme. | Required |
| Only Enable TFTP Server if Absolutely Necessary | TFTP is typically used for network booting of diskless workstations, X-terminals, and other similar devices. It is also used if a Kickstart server is present in the environment. | Required |
| Only Enable IMAP if Absolutely Necessary | Remote mail clients (like Eudora, Netscape Mail and Kmail) may retrieve mail from remote mail servers using IMAP, the Internet Message Access Protocol, or POP, the Post Office Protocol. | Required |
| Only Enable POP if Absolutely Necessary | Remote mail clients (like Eudora, Netscape Mail and Kmail) may retrieve mail from remote mail servers using IMAP, the Internet Message Access Protocol, or POP, the Post Office Protocol. | Required |
| **MINIMIZE BOOT SERVICES** | **Description** | **Action** |
| Set Daemon umask | The system default umask should be set to at least 027 in order to prevent daemon processes (such as the syslog daemon) from creating world-writable files by default. | Optional |
| Disable xinetd, If Possible | If possible completely disable the xinetd service on the system. | Required |
| Disable sendmail Server, If Possible | If a server is not acting as a mail server the sendmail daemon can be disabled. | Required |
| Disable GUI Login | Disable X Windows and GUI-based logins | Required |
| Disable X Font Server | If the X Windows Server is not being used you should also disable the X Font Server. | Required |
| Disable Standard Boot Services | Each system daemon that does not have a clear and necessary purpose on the host should be deactivated. | Optional |
| Only Enable SMB (Windows File Sharing) Processes If Absolutely Necessary | Red Hat Linux includes the popular Open Source Samba server for providing file and print services to Windows-based systems. This allows a Unix system to act as a file or print server in on a Windows network, and even act as a Domain Controller (authentication server) to older Windows operating systems. However, if this functionality is not required by the site, the service should be disabled. | Required |
| Only Enable NFS Server Processes If Absolutely Necessary | NFS is frequently exploited to gain unauthorized access to files and systems. | Required |
| Only Enable NFS Client Processes If Absolutely Necessary | NFS is frequently exploited to gain unauthorized access to files and systems. | Required |
| Only Enable NIS Client Processes If Absolutely Necessary | Unless this site must use NIS, it should really be avoided. While it can be very useful for transparently scaling the number of workstations, it's not well designed for security. | Required |
| Only Enable NIS Server Processes If Absolutely Necessary | Unless this site must use NIS, it should be avoided. While it can be very useful for transparently scaling the number of workstations, it is not well designed for security. | Required |
| Only Enable RPC Portmap Processes If Absolutely Necessary | RPC-based services typically use very weak or non-existent authentication and yet may share very sensitive information. | Required |
| Only Enable netfs Script If Absolutely Necessary | If there are no network file sharing protocols being used, one can deactivate the netfs script. This script mounts network drives on the client. | Required |
| Only Enable Printer Daemon Processes If Absolutely Necessary | If users will never print files from this machine and the system will never be used as a print server by other hosts on the network, then it is safe to disable the print daemon, lpd or cupsd. | Required |
| Only Enable Web Server Processes If Absolutely Necessary | Unfortunately web servers tend to be enabled on many systems that don’t need the web service, and are often not properly secured and administered. | Required |
| Only Enable SNMP Processes If Absolutely Necessary | If SNMP is used to monitor the hosts on this network, experts recommend changing the default community string used to access data via SNMP. | Required |
| Only Enable DNS Processes If Absolutely Necessary | BIND DNS has been widely implemented but has also had a history of security flaws. | Required |
| Only Enable SQL Server Processes If Absolutely Necessary | If your server does not need to run the mainstream database (SQL) servers Postgres or MySQL, it is safe to deactivate them. | Required |
| Only Enable Webmin Processes If Absolutely Necessary | One can remotely administer a system through the relatively safe SSH remote shell system. Webmin, and other tools like it, can be dangerous as they have a history of bad authentication or session management. | Required |
| Only Enable SQUID Caching Server if Absolutely Necessary | Squid can actually be beneficial to security, as it imposes a proxy between the client and server. On the other hand, if it is not being used, it should be deactivated and removed. | Required |
| Only Enable Kudzu Hardware Detection if Absolutely Necessary | Kudzu is Red Hat's hardware detection program, which is normally set to run during system startup. It detects changes in hardware and, without demanding authentication of any sort, allows the user at the console to configure that hardware. This lack of authentication presents the primary danger – any user sitting at the console during a reboot can configure any new devices added to the system. | Required |
| **KERNEL TUNING** | **Description** | **Action** |
| Network Parameter Modifications | Modification of configuration file that sets network parameters at boot time. | Required |
| Additional Network Parameter Modifications | Further modification of configuration file that sets network parameters at boot time. | Required |
| **LOGGING** | **Description** | **Action** |
| Capture Messages Sent To Syslog AUTHPRIV Facility | The default installation of Red Hat Enterprise Linux already has this enabled. It is included in case it had been previously disabled. | Required |
| Turn On Additional Logging For FTP Daemon | Whereas FTP is a more vulnerable protocol in a security sense, additional logging for the ftp daeamon should be configured. | Required |
| Confirm Permissions On System Log Files | Protect system log files from being modified by unauthorized individuals by confirming log file permissions on a regular basis. | Required |
| Install Splunk | Install and configure Splunk | Required |
| **FILE/DIRECTORY PERMISSIONS/ACCESS** | **Description** | **Action** |
| Add 'nodev' Option To Appropriate Partitions In /etc/fstab | Placing "nodev" on these partitions prevents users from mounting unauthorized devices on any partitions that we know should not contain devices. There should be little need to mount devices on any partitions other than /dev. | Optional |
| Add 'nosuid' and 'nodev' Option For Removable Media In /etc/fstab | Removable media is one vector by which malicious software can be introduced onto the system. By forcing these file systems to be mounted with the nosuid option, the administrator prevents users from bringing set-UID programs onto the system via CDROMs and floppy disks. | Required on Physical Hardware |
| Disable User-Mounted Removable File Systems | Disable the ability of regular users to mount removable file systems. | Required |
| Verify passwd, shadow, and group File Permissions | The file permissions for passwd, shadow, and group should be periodically checked. | Required |
| World-Writable Directories Should Have Their Sticky Bit Set | When the sticky-bit is set on a directory, only the owner of a file can remove that file from the directory, preventing users from overwriting each other’s files. | Required |
| Find Unauthorized World-Writable Files | Data in world-writable files can be modified and compromised by any user on the system. | Required |
| Find Unauthorized SUID/SGID System Executables | Administrators should ensure no rogue set-UID programs are introduced into systems. | Required |
| Find All Unowned Files | Unowned files should not be allowed and, if present, may be an indication an intruder has accessed the system. | Required |
| Disable USB Devices | PCMCIA cards, USB drives and memory devices represent another attack vector against your systems. The prices for a 512MB or even 1GB USB memory device have become very affordable, and is enough storage to transport vast quantities of data off a system. | Optional |
| **SYSTEM ACCESS, AUTHENTICATION, AND AUTHORIZATION** | **Setting** | **Adjustment** |
| Remove .rhosts Support In PAM Configuration Files | Used in conjunction with the BSD-style "r-commands" (rlogin, rsh, rcp), the .rhosts files implement a weak form of authentication based on the network address or host name of the remote computer (which can be spoofed by a potential attacker to exploit the local system). s and other network security elements should actually block rlogin/rsh/rcp access from external hosts. | Required |
| Create ftpusers Files | /etc/ftpusers and /etc/vsftp.ftpusers contain a list of users who are not allowed to access the system via FTP—there should be no reason for “system” type accounts to be transferring information via FTP and certainly root should not be used to transfer files via ftp. | Don't enable FTP |
| Prevent X Server From Listening on Port 6000/tcp | X servers listen on port 6000/tcp for messages from remote clients running on other systems. X Windows users a relatively insecure authentication protocol and an attacker who is able to gain authorized access to the local X server can easily compromise the system. | Don't enable X |
| Restrict at/cron To Authorized Users | The cron.allow and at.allow files are a list of users who are allowed to run the crontab and at commands to submit jobs to be run at scheduled intervals. | Required |
| Restrict Permissions On crontab files | The system crontab files are accessed only by the cron daemon (which runs with superuser priveleges) and the crontab command (which is set-UID to root). Allowing unprivileged users to read or (even worse) modify system crontab files can create the potential for a local user on the system to gain elevated priveleges. | Required |
| Configure xinetd Access Control | Configure xinetd to use simple IP-based access control and log connections. | Required if xinetd is installed |
| Restrict Root Logins to System Console | Anonymous root logins should never be allowed, except on the system console in emergency situations. | Required |
| Set LILO/GRUB Password | By default on most Linux systems, the boot loader prompt allows an attacker to subvert the normal boot process very easily. Adding a boot loader password adds and extra layer of security. | Optional |
| Require Authentication for Single-User Mode | By default on Red Hat Linux, you can enter single user mode simply by typing “linux single” at the LILO prompt or in the GRUB boot-editing menu. | Optional - Suggested |
| Restrict NFS Client Requests to Privileged Ports | Setting the secure parameter causes the NFS server process on the local system to ignore NFS client requests that do not originate from the privileged port range (ports less than 1024). | Required |
| Only enable syslog to Accept Messages If Absolutely Necessary | By default the system logging daemon, syslogd, does not listen for log messages from other systems on the network port 514/udp. It is a considered a “good practice” to setup a central log server but if a server is not a central log server, it should not be listening on port 514/udp. | Remove from list |
| **USER ACCOUNTS AND ENVIRONMENT** |  |  |
| Block System Accounts | Non-human system accounts should be made less useful to an attacker by locking them and setting the shell to a shell not in /etc/shells. | Required |
| Verify That There are No accounts with Empty Password Fields | An account with an empty password field means that anybody may log in as that user without providing a password at all. All account should have strong passwords. | Required |
| Set Account Expiration Parameters On Active Accounts | Force users to change passwords every 90 days, prevent password changes for seven days thereafter. | Required -Kerberos should enforce account expiration |
| Verify No Legacy ‘+’ Entries Exist In passwd, shadow, And group Files | ‘+’ entries in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries may provide an avenue for attackers to gain privileged access on the system, and should be deleted if they exist. | Optional |
| No ‘.’ Or Group/World-Writable Directory in Root’s $PATH | Including the current working directory (‘.’) or other writable directory in root’s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan Horse program. | Required |
| User Home Directories Should Be Mode 750 or More Restrictive | Group or World-Writable user home directories may enable malicious users to steal or modify other users’ data or to gain another user’s system privileges. | Required |
| No User Dot-Files Should Be World-Writable | World-writable user configuration files may enable malicious users to steal or modify other users’ data or to gain another users’ system privileges. | Required |
| Remove User .netrc Files | .netrc files may contain unencrypted passwords which may be used to attack other  systems. | Required |
| Set Default umask For Users | A default umask setting of 077—files and directories created by users will not be readable by any other system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system. | Required |
| Disable core dumps | Core dumps can consume large amounts of disk space and may contain sensitive data. | Required |
| Limit Access To The Root Account From su | Limit the amount of people who can access the root account via ‘su’. | Required - su or ksu |

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Review the configuration settings on the Redhat Linux server | * Confirm from the standard if the configuration settings on the server are the same |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework.*

## Glossary / Acronyms

|  |  |
| --- | --- |
| syslog | System Log |
| FTP | File Transfer Protocol |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Distribution

* *Information Security*
* *IT Department*