SUPPORTED IMAGES

Core STIG Hardening

Linux Hardening Changes and Operational Reference

Applies to harden-linux.sh Version 1.0

```
ENABLE_FIREWALL=1 ALLOW_TCP_PORTS="22" sudo ./harden-linux.sh
```

Supported operating systems

Debian | Ubuntu | RHEL | CentOS Stream | AlmaLinux | Rocky Linux | Oracle Linux

Supported Images LLC

Document date: August 21, 2026

Scope note

"Supported Images Core STIG Hardening" is the name used in this document for the baseline implemented by the supplied script. It applies STIG-oriented core hardening controls, but this document does not represent a claim that a system is fully compliant with every requirement of a particular DISA STIG release. Formal STIG compliance requires system-role-specific review, exceptions, evidence, and validation.

1. Purpose and Execution Summary

The Supported Images Core STIG Hardening script provides a common unattended security baseline across Debian/Ubuntu and RHEL-family Linux distributions. The script detects the operating system, selects the appropriate package-management and security-control path, applies shared kernel and service hardening, records status information, and reports whether a reboot is required.

This document describes the changes expected when the script is launched with:

```
ENABLE_FIREWALL=1 ALLOW_TCP_PORTS="22" sudo ./harden-linux.sh
```

Important sudo environment note

The command above assumes the sudo configuration preserves ENABLE_FIREWALL and ALLOW_TCP_PORTS from the caller environment. On systems where sudo resets these variables, use the more reliable form: sudo env ENABLE_FIREWALL=1 ALLOW_TCP_PORTS="22" ./harden-linux.sh. The remainder of this document assumes the script receives ENABLE_FIREWALL=1 and ALLOW_TCP_PORTS="22".

Firewall requested	Yes (ENABLE_FIREWALL=1)
Requested inbound TCP port	22/TCP
Requested inbound UDP ports	None
SSH port	22/TCP (default SSH_PORT=22)
Automatic updates	Enabled by default
MAC framework	AppArmor on Debian/Ubuntu; SELinux on RHEL-family systems
Audit logging	Enabled by default
Fail2ban	Enabled by default when package/tooling is available
Strict SSH algorithms	Enabled by default
Profile/session hardening	Enabled by default
Kernel-module restrictions	Enabled by default
/tmp noexec hardening	Disabled by default
AIDE	Disabled by default

2. System Detection, Logging, and Backups

2.1 Operating-system detection

The script reads /etc/os-release and routes the host into one of two security-control families:

- Debian family: Debian and Ubuntu, with ID_LIKE fallback for Debian-compatible derivatives.
- RHEL family: RHEL, CentOS Stream, AlmaLinux, Rocky Linux, and Oracle Linux, with ID_LIKE fallback for RHEL/Fedora-compatible derivatives.
- Unsupported distributions cause the script to stop rather than apply an assumed hardening path.

2.2 Package-manager selection

- Debian/Ubuntu: apt-get.
- RHEL family: dnf when present; otherwise yum.
- On the RHEL-family path, the current script attempts to install epel-release during package-manager setup. This is intended to make packages such as Fail2ban available where EPEL is supported.

2.3 Backup location

Existing configuration files explicitly passed through the script's backup helper are copied before modification to a timestamped directory under:

```
/root/hardening-backups/YYYYMMDDTHHMMSSZ/
```

Examples include SSH configuration, automatic-update configuration, SELinux configuration, sysctl settings, core-dump settings, Fail2ban configuration, audit rules, and firewall configuration where the relevant function invokes the backup helper.

2.4 System hardening log

Primary hardening log

By default, the script writes its action messages, warnings, detected platform information, and final hardening/status inventory to /var/log/system-hardening.log. The file is created with mode 0600, so root privileges are normally required to read it.

```
sudo less /var/log/system-hardening.log

sudo tail -n 200 /var/log/system-hardening.log
```

The log is the primary place to review what the hardening script attempted and the resulting status. Package-manager commands may also produce detailed output directly on the terminal; that console output is not necessarily duplicated line-for-line in system-hardening.log.

3. Package and Update Changes

The script refreshes package metadata, installs available security tooling, and performs a system package upgrade before applying the configuration controls below.

3.1 Debian / Ubuntu

- Refreshes APT metadata with apt-get update.
- Installs ca-certificates when available.
- Installs unattended-upgrades because automatic updates are enabled by default.
- Installs AppArmor and apparmor-utils when available.
- Installs auditd and Fail2ban when available.
- Installs nftables because ENABLE_FIREWALL=1.
- Runs a non-interactive apt-get upgrade while retaining existing local package configuration where dpkg encounters configuration-file choices.

3.2 RHEL / CentOS Stream / AlmaLinux / Rocky / Oracle Linux

- Attempts to install epel-release during package-manager setup.
- Refreshes repository metadata with dnf/yum makecache.
- Installs ca-certificates when available.
- Installs dnf-automatic when dnf is used, or yum-cron when the yum path is used, because automatic updates are enabled by default.
- Installs audit, Fail2ban when available, and firewalld because ENABLE_FIREWALL=1.
- Installs dnf-plugins-core on dnf systems or yum-utils on yum systems to support reboot/restart checks when available.
- Applies all available package upgrades from enabled repositories using dnf upgrade --refresh or yum update.

3.3 Ongoing automatic updates

- Debian/Ubuntu: writes /etc/apt/apt.conf.d/20auto-upgrades, enables periodic package-list refresh, unattended upgrades, and a 7-day autoclean interval, then enables/starts apt-daily and apt-daily-upgrade timers.
- DNF systems: enables dnf-automatic-install.timer when present; otherwise configures/enables dnf-automatic.timer and sets apply_updates=yes when the setting is available.

- YUM systems: updates /etc/yum/yum-cron.conf to download/apply updates and enables yum-cron.service.

4. Mandatory Access Control

4.1 Debian / Ubuntu - AppArmor

- Installs AppArmor tooling when available.
- Enables and starts apparmor.service when that service unit exists.
- Runs aa-status and logs a warning if AppArmor is not fully active.

4.2 RHEL family - SELinux

- If SELinux is Enforcing, no mode change is made.
- If SELinux is Permissive, /etc/selinux/config is backed up and changed to SELINUX=enforcing, then setenforce 1 is attempted immediately.
- If SELinux is Disabled, it remains disabled because ENABLE_DISABLED_SELINUX defaults to 0. The script only schedules enablement/relabeling when that separate toggle is explicitly set to 1.

5. Kernel and Network Hardening

The script creates or replaces /etc/sysctl.d/99-system-hardening.conf, sets mode 0600, and attempts to apply the values immediately. The settings are:

Setting	Effect
kernel.randomize_va_space = 2	Full address-space layout randomization (ASLR).
kernel.kptr_restrict = 2	Restricts kernel pointer exposure.
kernel.dmesg_restrict = 1	Restricts access to kernel messages.
kernel.perf_event_paranoid = 2	Restricts unprivileged performance-event access.
kernel.yama.ptrace_scope = 1	Restricts ptrace to reduce cross-process inspection.
kernel.unprivileged_bpf_disabled = 1	Disables unprivileged BPF use where supported.
kernel.sysrq = 0	Disables the SysRq interface.
net.core.bpf_jit_harden = 2	Enables BPF JIT hardening for all users where supported.
fs.suid_dumpable = 0	Disables core dumps for setuid/setgid programs.
net.ipv4.conf.all/default.accept_redirects = 0	Rejects IPv4 ICMP redirects.
net.ipv4.conf.all/default.secure_redirects = 0	Rejects “secure” IPv4 redirects.
net.ipv4.conf.all/default.send_redirects = 0	Prevents the host from sending IPv4 redirects.
net.ipv4.conf.all/default.accept_source_route = 0	Rejects IPv4 source-routed packets.
net.ipv4.conf.all/default.log_martians = 1	Logs suspicious/martian IPv4 packets.
net.ipv4.conf.all/default.rp_filter = 1	Enables strict IPv4 reverse-path filtering.

Setting	Effect
net.ipv4.icmp_echo_ignore_broadcasts = 1	Ignores broadcast ICMP echo requests.
net.ipv4.icmp_ignore_bogus_error_responses = 1	Ignores bogus ICMP error responses.
net.ipv4.tcp_syncookies = 1	Enables TCP SYN cookies.
net.ipv4.tcp_rfc1337 = 1	Enables protection against TIME-WAIT assassination behavior.
net.ipv6.conf.all/default.accept_redirects = 0	Rejects IPv6 redirects.
net.ipv6.conf.all/default.accept_source_route = 0	Rejects IPv6 source routing.

Compatibility consideration
Strict reverse-path filtering (rp_filter=1) can require review on hosts using asymmetric routing, some multi-homed designs, advanced VPN/routing configurations, or certain cloud networking patterns.

6. Core Dump Restrictions

- Writes /etc/security/limits.d/99-system-hardening.conf with hard core limits of 0 for all users and root.
- Writes /etc/systemd/coredump.conf.d/99-system-hardening.conf with Storage=none and ProcessSizeMax=0.
- Runs systemctl daemon-reload.

7. OpenSSH Hardening

If the OpenSSH server is installed, the script backs up the main SSH configuration and its managed drop-in, ensures /etc/ssh/sshd_config.d exists, normalizes the standard Include directive to the beginning of sshd_config, and creates /etc/ssh/sshd_config.d/00-hardening.conf with mode 0600.

7.1 Settings always written when SSH is present

- Port 22
- PermitEmptyPasswords no
- HostbasedAuthentication no
- IgnoreRhosts yes
- X11Forwarding no
- MaxAuthTries 3
- LoginGraceTime 30
- ClientAliveInterval 300
- ClientAliveCountMax 2
- LogLevel VERBOSE
- PermitUserEnvironment no

7.2 Conditional public-key enforcement

The script scans /root/.ssh and /home for non-empty authorized_keys files containing recognized SSH public-key types.

- If a usable public key is found: PermitRootLogin prohibit-password is written.
- Because DISABLE_SSH_PASSWORDS_IF_KEYS defaults to 1, PasswordAuthentication no, KbdInteractiveAuthentication no, and ChallengeResponseAuthentication no are also written when a usable key is found.
- If no usable key is detected, the script deliberately does not force those password/root-login settings, reducing the risk of an unattended SSH lockout.

7.3 Strict SSH algorithms

ENABLE_STRICT_SSH_CIPHERS defaults to 1, so the script also writes explicit key-exchange, cipher, and MAC allowlists:

```
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com
```

SSH safety behavior

The script runs sshd -t before reloading SSH. If validation fails, it restores the prior SSH configuration backup and validates the restored configuration. This protects against leaving sshd with a syntactically invalid managed configuration.

8. Fail2ban and Audit Logging

8.1 Fail2ban

- Creates /etc/fail2ban/jail.d/99-system-hardening.local when Fail2ban and sshd are available.
- Enables the sshd jail on port 22.
- Sets maxretry=5, findtime=10m, and bantime=1h.
- Tests the Fail2ban configuration before restarting the service. If the test fails, the managed jail file is removed.

8.2 auditd

The script writes /etc/audit/rules.d/99-system-hardening.rules and monitors security-sensitive configuration and execution activity, including:

- /etc/passwd, /etc/group, /etc/shadow, and /etc/gshadow changes.
- /etc/sudoers and /etc/sudoers.d changes.
- /etc/ssh/sshd_config and /etc/ssh/sshd_config.d changes.
- /etc/modprobe.d changes.
- /etc/selinux/config and/or /etc/apparmor.d changes when present.
- /etc/localtime changes.
- Execution of /usr/bin/sudo.
- All execve system calls for b64 and b32 audit architectures.

Audit-volume consideration

Auditing every execve call can generate a large volume of audit records on busy systems. Capacity, log rotation, forwarding, and SIEM ingestion should be sized accordingly.

9. File, Session, and Kernel-Module Hardening

9.1 File permissions

- Removes all group/other permissions from /etc/shadow and /etc/gshadow.
- Removes group/other write permission from /etc/passwd and /etc/group.
- Sets /root to mode 0700.
- Removes group/other write permission from files under /etc/cron.d and the hourly/daily/weekly/monthly cron directories.

9.2 Global profile/session settings

- Writes /etc/profile.d/99-hardening-umask.sh containing umask 027.

- Writes /etc/profile.d/99-hardening-tmout.sh with readonly TMOUT=900 and export TMOUT, establishing a 15-minute idle timeout for compatible interactive shells that process /etc/profile.d.

Operational note
The profile hardening files are written directly by the function. Existing files with these exact names would be replaced.

9.3 Kernel-module restrictions

The script creates modprobe configuration files that redirect loading of the following modules to /bin/true:

- Filesystems: cramfs, freevxfs, jffs2, hfs, hfsplus, squashfs, udf.
- USB storage: usb-storage.
- Network protocols: dccp, sctp, rds, tipc.
- vfat is intentionally not disabled, to avoid breaking UEFI boot partitions commonly used in AWS images.

Compatibility consideration
Disabling squashfs can affect software that depends on SquashFS images (for example, some Snap-based application deployments on Ubuntu). Disabling usb-storage prevents future use of USB mass-storage devices once the module restriction takes effect.

10. Firewall Behavior for ALLOW_TCP_PORTS="22"

ENABLE_FIREWALL=1 selects the distribution-specific host firewall. ALLOW_TCP_PORTS="22" requests TCP port 22. ALLOW_UDP_PORTS remains empty by default.

10.1 Debian / Ubuntu: nftables

- Installs nftables if needed.
- Before changing the firewall, checks whether any nftables tables already exist.
- Because REPLACE_EXISTING_NFTABLES defaults to 0, an existing nftables ruleset causes the firewall hardening step to be skipped. The existing rules remain intact.
- If no existing nftables tables are found, the script backs up /etc/nftables.conf and creates a managed ruleset.
- The managed INPUT chain uses policy drop.
- Allows established/related traffic and loopback traffic; drops invalid connection states.
- Allows IPv4 ICMP and IPv6 ICMP traffic.
- Allows DHCP client traffic (UDP 67→68 and UDP 547→546).
- Allows new inbound TCP connections to port 22.
- No additional inbound UDP application ports are allowed by ALLOW_UDP_PORTS.
- The FORWARD chain uses policy drop; the OUTPUT chain uses policy accept.
- Validates the generated ruleset with nft -c before installing it, writes /etc/nftables.conf with mode 0600, loads it, and enables/restarts nftables.service.

Debian/Ubuntu firewall result
When the host starts with no existing nftables tables, this invocation produces a restrictive managed firewall whose only configured inbound TCP application port is 22. If an nftables ruleset already exists, the script does not replace it with this command.

10.2 RHEL family: firewalld

- Installs firewalld if needed and enables/starts firewalld.service.
- If nftables.service is already active while firewalld is inactive, the script stops rather than introduce a competing firewall manager.
- If FIREWALL_ZONE is not specified and exactly one active firewalld zone exists, that active zone is selected.
- If multiple active zones exist, the script stops and requires FIREWALL_ZONE to be explicitly specified.
- If no active zone exists, the firewalld default zone is selected.
- Adds permanent 22/tcp permission to the selected zone and reloads firewalld.

- Existing firewalld services, ports, rich rules, and other rules are preserved.

RHEL-family firewall result

ALLOW_TCP_PORTS="22" adds port 22/TCP; it does not mean port 22 becomes the only allowed inbound port. Existing firewalld rules are intentionally preserved.

11. Controls Not Enabled by This Invocation

- Filesystem /tmp hardening is OFF because ENABLE_FS_HARDENING defaults to 0. Therefore the script does not create/enable the tmp.mount configuration that would mount /tmp as tmpfs with nosuid,nodev,noexec.
- AIDE is OFF because ENABLE_AIDE defaults to 0. No AIDE package installation or database initialization is performed by this invocation.
- Completely disabled SELinux is not re-enabled because ENABLE_DISABLED_SELINUX defaults to 0.
- On Debian/Ubuntu, an existing nftables ruleset is not replaced because REPLACE_EXISTING_NFTABLES defaults to 0.

12. Final Status Collection and Reboot Indication

At the end of a successful run, the script appends a status inventory to /var/log/system-hardening.log. Depending on the platform and installed tooling, this includes:

- Kernel and detected distribution/version/family.
- Package manager selected by the script.
- AppArmor status on Debian/Ubuntu.
- SELinux status and system crypto policy on RHEL-family systems.
- Effective SSH settings, including port, authentication settings, key exchange algorithms, ciphers, and MACs.
- auditd status.
- Fail2ban sshd jail status.
- nftables or firewalld status when firewall hardening was requested.
- Listening TCP/UDP sockets.
- World-writable directories on the root filesystem (informational list, capped by the script).
- SUID/SGID files on the root filesystem (informational list, capped by the script).
- Automatic-update service/timer status.

The script also checks whether the platform indicates that a reboot is required or recommended and writes a warning to the hardening log when applicable.

13. Recommended Post-Run Review

1. Review the primary hardening log:

```
sudo less /var/log/system-hardening.log
```

2. Confirm the effective SSH configuration before ending the current administrative session:

```
sudo sshd -T | egrep '^(port|permitrootlogin|passwordauthentication|kbdinteractiveauthentication|kexalgorithms|ciphers|macs) '
```

3. Review firewall state:

```
sudo nft list ruleset              # Debian / Ubuntu
sudo firewall-cmd --list-all       # RHEL family
```

4. Verify MAC enforcement:

```
sudo aa-status                  # Debian / Ubuntu
sudo getenforce                 # RHEL family
```

5. Review Fail2ban and audit status:

```
sudo fail2ban-client status sshd
sudo auditctl -s
```

6. If the log reports a required/recommended reboot, reboot according to the system's maintenance policy and re-check SSH, firewall, MAC, and application functionality afterward.

14. Key Files Created or Modified

Path / Object	Purpose
/var/log/system-hardening.log	Primary action/status log; mode 0600.
/root/hardening-backups/<timestamp>/	Timestamped backups for files processed by backup_file().
/etc/sysctl.d/99-system-hardening.conf	Kernel and network sysctl baseline.
/etc/security/limits.d/99-system-hardening.conf	Core-dump hard limit.
/etc/systemd/coredump.conf.d/99-system-hardening.conf	Disables systemd-coredump storage/processing.
/etc/ssh/sshd_config.d/00-hardening.conf	Managed SSH hardening settings.
/etc/fail2ban/jail.d/99-system-hardening.local	Managed Fail2ban sshd jail.
/etc/audit/rules.d/99-system-hardening.rules	Managed auditd rules.
/etc/profile.d/99-hardening-umask.sh	Global umask 027.
/etc/profile.d/99-hardening-tmout.sh	15-minute shell idle timeout.
/etc/modprobe.d/disable-*.conf	Kernel filesystem/protocol/USB-storage module restrictions.
/etc/apt/apt.conf.d/20auto-upgrades	Debian/Ubuntu automatic-update schedule/settings.
/etc/dnf/automatic.conf	May be modified on RHEL-family dnf systems using dnf-automatic.timer fallback.
/etc/yum/yum-cron.conf	May be modified on yum-based systems.
/etc/nftables.conf	Debian/Ubuntu managed firewall when no existing nftables rules are present.
firewalld permanent zone configuration	RHEL-family firewall is updated through firewall-cmd; existing rules are preserved.

Appendix A - Default Toggle Values Relevant to This Run

ENABLE_AUTO_UPDATES	1 - enabled
ENABLE_MAC	1 - enabled
ENABLE_AUDITD	1 - enabled
ENABLE_FAIL2BAN	1 - enabled
ENABLE_FIREWALL	1 - explicitly enabled by this invocation
HARDEN_SSH	1 - enabled

DISABLE_SSH_PASSWORDS_IF_KEYS	1 - enabled conditionally when a usable key is detected
DISABLE_CORE_DUMPS	1 - enabled
ENABLE_DISABLED_SELINUX	0 - disabled
REPLACE_EXISTING_NFTABLES	0 - disabled
ENABLE_STRICT_SSH_CIPHERS	1 - enabled
ENABLE_PROFILE_HARDENING	1 - enabled
ENABLE_MODULE_HARDENING	1 - enabled
ENABLE_FS_HARDENING	0 - disabled
ENABLE_AIDE	0 - disabled
SSH_PORT	22
ALLOW_TCP_PORTS	22 - explicitly set by this invocation
ALLOW_UDP_PORTS	empty

Source basis: Supported Images LLC harden-linux.sh, Version 1.0, dated 2026-08-20. This guide describes the behavior implemented in the supplied script and the default values present in that version.