

Audit Monitoring Commands

This module describes the audit monitoring commands available on the router. These commands are used to proactively monitor the security and compliance of the router by enabling audit monitoring.

For detailed information about system health check concepts, configuration tasks, and examples, see the *Implementing Audit Monitoring* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

- linux security audit, on page 1
- show linux security audit, on page 5

linux security audit

To enable the Linux audit monitoring and logging capabilities, use the **linux security audit** command in XR Config mode. Use the **no** form of the command to disable the configuration.

linux security audit { **monitor** { **all** | **authlog-files** | **cron-files** | **dns-client-files** | **docker** | **file-deletion** | **file-perm-changes** | **kernel-module-mgmt** | **process-audits** | **system-login-reboot** | **system-software** | **system-time-change** | **user-group-config-files** | **user-privilege-mgmt** | **xr-software** | **logging** | **syslog** | **keepalive interval** *interval* } }

Syntax Description

monitor	Enable audit monitoring.
all	Enable audit monitoring for all rule groups.
authlog-files	Enable audit monitoring for changes in authlog files.
cron-files	Enable audit monitoring for changes in cron files.
dns-client-files	Enable audit monitoring for changes in DNS client files.
docker	Enable audit monitoring for changes in docker.
file-deletion	Enable audit monitoring for file deletion.
file-perm-changes	Enable audit monitoring for changes in file permissions.
kernel-module-mgmt	Enable audit monitoring for kernel module management.
process-audits	Enable audit monitoring for process audits.

system-login-reboot	Enable audit monitoring for system login and reboot.
system-software	Enable audit monitoring for changes in system software.
system-time-change	Enable audit monitoring for changes in system time.
user-group-config-files	Enable audit monitoring for changes in user group configuration files.
user-privilege-mgmt	Enable audit monitoring for changes in user privileges.
xr-software	Enable audit monitoring for changes in IOS XR software.
logging syslog	Enable forwarding of audit logs to a remote syslog server.
keepalive interval *interval*	Enables AuditD process keepalive and sets the keepalive interval in minutes.

Command Default

Audit monitoring is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 26.3.1	Two new options, **keepalive** and **interval**, were added to the command.
Release 25.3.1	This command was introduced.

Usage Guidelines

The router stores audit logs locally at **/var/log/audit/audit.log**, unless you enable log forwarding.

The table lists the rules within each of the rule-groups.

Rule-group	Rules
xr-software	-a always,exit -F arch=b64 -F dir=/pkg/bin -F perm=wa -k xr_bin_changes -a always,exit -F arch=b64 -F dir=/pkg/sbin -F perm=wa -k xr_sbin_changes -a always,exit -F arch=b64 -F dir=/pkg/lib -F perm=wa -k xr_lib_changes
user-group-config-files	-a always,exit -F arch=b64 -F path=/etc/passwd -F perm=wa -k passwd_changes -a always,exit -F arch=b64 -F path=/etc/shadow -F perm=wa -k shadow_changes -a always,exit -F arch=b64 -F path=/etc/group -F perm=wa -k group_changes -a always,exit -F arch=b64 -F path=/etc/sudoers -F perm=wa -k sudoers_changes

Rule-group	Rules
dns-client-files	-a always,exit -F arch=b64 -F path=/etc/hosts -F perm=wa -k hosts_changes -a always,exit -F arch=b64 -F path=/etc/resolv.conf -F perm=wa -k dns_changes -a always,exit -F arch=b64 -F path=/var/run/resolv.conf -F perm=wa -k dns_changes
authlog-files	-a always,exit -F arch=b64 -F path=/var/log/auth.log -F perm=wa -k authlog_changes
system-time-change	-a always,exit -F arch=b64 -F path=/etc/localtime -F perm=wa -k time_changes
system-login-reboot	-a always,exit -F arch=b64 -F path=/var/log/wtmp -F perm=wa -k shutdown_reboot
cron-files	-a always,exit -F arch=b64 -F path=/etc/crontab -F perm=wa -k cron_changes -a always,exit -F arch=b64 -F dir=/etc/cron.d -F perm=wa -k cron_changes -a always,exit -F arch=b64 -F dir=/etc/cron.daily -F perm=wa -k cron_changes -a always,exit -F arch=b64 -F dir=/etc/cron.hourly -F perm=wa -k cron_changes -a always,exit -F arch=b64 -F dir=/etc/cron.weekly -F perm=wa -k cron_changes -a always,exit -F arch=b64 -F dir=/etc/cron.monthly -F perm=wa -k cron_changes
kernel-module-mgmt	-a always,exit -F arch=b64 -F path=/sbin/insmod -F perm=x -k modules -a always,exit -F arch=b64 -F path=/sbin/rmmod -F perm=x -k modules -a always,exit -F arch=b64 -F path=/sbin/modprobe -F perm=x -k modules -a always,exit -F arch=b64 -F path=/usr/bin/kmod -F perm=x -k modules
system-software	-a always,exit -F arch=b64 -F dir=/bin -F perm=wa -k bin_changes -a always,exit -F arch=b64 -F dir=/sbin -F perm=wa -k sbin_changes -a always,exit -F arch=b64 -F dir=/usr/bin -F perm=wa -k usr_bin_changes -a always,exit -F arch=b64 -F dir=/usr/sbin -F perm=wa -k usr_sbin_changes

Rule-group	Rules
docker	-a always,exit -F arch=b64 -F path=/lib/systemd/system/docker.service -F perm=wa -k docker_service -a always,exit -F arch=b64 -F path=/lib/systemd/system/docker.socket -F perm=wa -k docker_socket -a always,exit -F arch=b64 -F path=/usr/bin/dockerd -F perm=xa -k docker_daemon -a always,exit -F arch=b64 -F path=/etc/docker/daemon.json -F perm=wa -k docker_config -a always,exit -F arch=b64 -F dir=/var/lib/docker -F perm=wa -k docker_storage -a always,exit -F arch=b64 -S execve -F path=/usr/bin/docker -k docker_commands
process-audits	-a always,exit -F arch=b64 -S execve -F auid>=1000 -F auid!=-1 -k process_audit
file-perm-changes	-a always,exit -F arch=b64 -S fchmodat -k file_perm_changes
user-privilege-mgmt	-a always,exit -F arch=b64 -S setuid,setresuid,setreuid,setfsuid,setgid,setresgid,setregid,setfsgid -k user_group_management
file-deletion	-a always,exit -F arch=b64 -S unlink,unlinkat -k file_deletion

This table provides the description of the various components of the rules:

Component	Description
-a	Action, e.g., `always,exit` means always log on exit of syscall
-F	Field match, e.g., `arch=b64` (architecture), `dir=`, `path=`, `perm=`, etc.
arch=b64	Architecture: 64-bit
dir=	Directory to monitor (e.g., `/pkg/bin`, `/etc/cron.d`)
path=	File to monitor (e.g., `/etc/passwd`, `/usr/bin/docker`)
perm=	Permissions watched: `r` (read), `w` (write), `x`(execute), `a` (attribute change)
-k	Key: Custom tag for easier filtering/searching in audit logs (e.g., `xr_bin_changes`, `cron_changes`)
-S	Syscall(s) to monitor (e.g., `execve`, `fchmodat`, `unlink`)
auid	Audit user ID; `auid>=1000` means all regular (non-system) users
always,exit	Log every time the rule is matched on syscall exit

Task ID

Task ID	Operation
network	read, write
interface	read, write
system	read, write

Example

This example shows how you can enable audit monitoring with the **linux security audit monitor** command.

```
Router# conf t
Router(config)# linux security audit monitor xr-software
Router(config)# linux security audit monitor user-group-config-files
Router(config)# commit
```

This example shows how you can enable audit log forwarding with the **linux security audit logging syslog** command.

```
Router# conf t
Router(config)# linux security audit logging syslog
Router(config)# logging 10.0.1.2 vrf default port 514
Router(config)# commit
```

This example shows how you can configure the AuditD process keepalive interval and enable remote audit log forwarding.

```
#Configure the AuditD process keepalive interval
Router# conf t
Router(config)# linux security audit keepalive interval 1010

#Enable remote audit log forwarding
Router(config)# linux security audit logging syslog
Router(config)# commit
```

show linux security audit

To view the details of the Linux security audit information, use the **show linux security audit** command in XR EXEC mode.

show linux security audit { **monitor status** { *rule-group* | **detail** *rule-group* } | **logging syslog** }

Syntax Description

monitor	Displays the audit monitor information.
status	Displays the audit monitor status.

rule-group	Displays the status of the specified rule group. This field can take these values: **all, authlog-files, cron-files, dns-client-files, docker, file-deletion, file-perm-changes, kernel-module-mgmt, process-audits, system-login-reboot, system-software, system-time-change, user-group-config-files, user-privilege-mgmt, xr-software**
detail	Displays the detailed status of the specified rule group.
logging	Displays the audit logging information.
syslog	Displays the remote syslog server information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

This table specifies the command usage:

Command	Description
`show linux security audit monitor status`	Shows all currently enabled rules.
`show linux security audit monitor status detail`	Shows all currently enabled rules with per-location status.
`show linux security audit monitor status`	Shows status and rules for any key (enabled or disabled).
`show linux security audit monitor status detail`	Shows per-location status for any key (enabled or disabled).
`show linux security audit logging syslog`	Shows syslog forwarding status and configured servers.

Task ID

Task ID	Operation
system	read

Example

The example displays the status of the audit rule-groups.

```
Router# show linux security audit monitor status
key name: xr-software                status: enabled
rules:
-a always,exit -F arch=b64 -F dir=/pkg/bin -F perm=wa -k xr_bin_changes
-a always,exit -F arch=b64 -F dir=/pkg/sbin -F perm=wa -k xr_sbin_changes
-a always,exit -F arch=b64 -F dir=/pkg/lib -F perm=wa -k xr_lib_changes
------------------------------------------------------------
key name: user-group-config-files    status: enabled
```

```
rules:
-a always,exit -F arch=b64 -F path=/etc/passwd -F perm=wa -k passwd_changes
-a always,exit -F arch=b64 -F path=/etc/shadow -F perm=wa -k shadow_changes
-a always,exit -F arch=b64 -F path=/etc/group -F perm=wa -k group_changes
-a always,exit -F arch=b64 -F path=/etc/sudoers -F perm=wa -k sudoers_changes
-----------------------------------------------------------------
```

This example displays the audit log forwarding details.

```
Router# show linux security audit logging syslog
status: enabled
syslog-server(s):
ipaddr: 10.0.1.2 vrf: default port: 514
ipaddr: 2001:db8::1 vrf: default port: 514
```