Implementing Audit Monitoring

TThis chapter explains the audit monitoring and logging capabilities available on NCS 1020 and how to configure audit monitoring.

Feature name	Release information	Description
Audit logging and monitoring	Cisco IOS XR 25.3.1	You can enable audit logging and monitoring on the NCS 1020. You can also configure predefined rule groups that allow NCS 1020 to monitor activities, log events, and, when necessary, forward audit logs to a remote syslog server for centralized analysis and incident response. This feature helps enhance security and compliance on your network. CLI: These new commands are introduced: • **linux security audit monitor***group-keyword* • **show linux security audit monitor status** • **linux security audit logging syslog** • • **logging** *remote-server-ip***vrf***remote-server-ip* • **show linux security audit logging syslog**

- Audit logging, on page 2
- AuditD process keepalive, on page 5

Audit logging

Audit logging is a security and compliance feature that

- operates according to defined audit rules automatically creating audit logs whenever specified actions or changes occur on the router
- integrates with the Linux Audit Daemon to monitor and log relevant security events across the router, and
- allows forwarding of audit logs to a remote syslog server.

Linux audit daemon is a user-space component of the Linux auditing system that

- tracks and logs system calls, file accesses, user actions, and other events as specified by audit rules, and
- provides administrators with insights to detect suspicious behavior and maintain system integrity.

An audit rule is a configuration that

- specifies which files, directories, or system events should be monitored
- determines the conditions for monitoring, and
- forms the foundation of an audit logging system.

An Audit log is a chronological record that

- is automatically generated when a monitored event, as defined by an audit rule, occurs, and
- typically includes details such as the event type, timestamp, user or process involved, and affected resources.

Audit rules and audit logs for security monitoring

Administrators define audit rules to track changes to sensitive files, monitor system calls, and observe other critical activities. By customizing audit rules, organizations can align monitoring with their unique security and compliance requirements.

Audit rules establish what to watch, while audit logs capture and document every relevant occurrence, ensuring a complete and actionable history of system activity.

For example, an audit rule that monitors changes to /etc/passwd file creates an audit log entry each time this file is modified.

Audit logging is not to be confused with system logging. While audit logging records security-relevant events, such as user actions and changes to sensitive files, system logging (syslog) captures general system events like service status updates, routine errors, or informational messages.

How audit logging works

Summary

These are the key components involved in this feature:

- Network Administrator: The user who initiates configurations via CLI.
- Linux audit daemon : The process that monitors system activity according to the installed rules and writes audit event logs.
- Local rsyslog daemon: The process that forwards logs to a remote syslog server.
- Remote syslog server: The external server that maintains the logs generated by the router.

The Linux audit daemon is the core service that actually performs event monitoring and logging, based on the audit rules configured by the administrator. It operates at the operating system level on each node, such as line cards and processors.

Workflow

These stages describe how audit monitoring and logging works.

1. The network administrator enables audit monitoring via CLI.
2. The router software receives the configurations, applies the relevant audit rules, and ensures these rules are distributed to all appropriate nodes.
3. On each node, the Linux audit daemon actively monitors system events as defined by the audit rules and writes the logs to a local log file at **/var/log/audit/audit.log**.
4. If the network administrator has enabled log forwarding, the audit logs are sent to the local rsyslog daemon, which then forwards the logs to a remote syslog server.

Guidelines for audit logging

Granularity of audit rules

- You can enable or disable audit rules only at the group level, not individually within a group.
- Regularly review the status of audit rules and audit log forwarding to ensure monitoring remains effective.

Resource usage on NCS 1020

Use caution when enabling all rule groups, especially those that monitor frequent events, as this may increase CPU, memory, or disk usage. Enable only the groups required for compliance or security needs.

Security of audit logs and syslog servers

- Allow only users with appropriate administrative privileges to configure or view Linux security audit settings.
- Protect access to audit logs and syslog servers to prevent unauthorized access or tampering.

Log forwarding to remote syslog servers

- Confirm that the remote syslog server is reachable and properly configured before enabling log forwarding.
- NCS 1020 forwards audit logs to remote syslog servers in unencrypted plain text. Use only trusted network segments for remote syslog servers.

Notes about audit log storage

- NCS 1020 stores audit logs locally at **/var/log/audit/audit.log**, unless you enable log forwarding.
- By default, the system rotates up to five audit log files, each up to 8 MB in size.

Configure audit logging

Follow this task to configure and monitor audit logs for specific system events by enabling the relevant audit rule groups.

Procedure

Step 1 Execute the **linux security audit monitor** <*group-keyword*> command, to enable a group of audit rules.

Example:

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# linux security audit monitor xr-software
RP/0/RP0/CPU0:ios(config)# linux security audit monitor user-group-config-files
RP/0/RP0/CPU0:ios(config)# commit
```

Step 2 Run the **show linux security audit monitor status** command, to verify the general status of all active audit rule groups.

Example:

```
RP/0/RP0/CPU0:ios# show linux security audit monitor status
Wed Aug 20 16:16:23.518 IST
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
------------------------------------------------------------
```

Step 3 (Optional) Execute the **linux security audit logging syslog** command, to enable forwarding of audit rules.

Example:

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# linux security audit logging syslog
RP/0/RP0/CPU0:ios(config)# commit
```

Step 4 (Optional) Execute the **logging** *remote-server-ip* **vrf** *vrf-name* command, to configure the remote syslog server.

Example:

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# logging 10.0.1.2 vrf default severity info port default facility local6
RP/0/RP0/CPU0:ios(config)# commit
```

Step 5 (Optional) Run the **show linux security audit logging syslog** command, to verify whether audit log forwarding is enabled and to view the configured remote syslog server.

Example:

```
RP/0/RP0/CPU0:ios# show linux security audit logging syslog
Wed Aug 20 16:16:44.553 IST
status: enabled
syslog-server(s):
ipaddr: 10.0.1.2 vrf: vrf-default port: 514
ipaddr: 10.0.1.9 vrf: vrf-default port: 514
```

AuditD process keepalive

AuditD process keepalive is a NCS 1020 capability that

- verifies the health of the Linux AuditD service by periodically generating keepalive events
- confirms that the audit logging path remains operational, and
- provides a positive audit signal for compliance and early detection of silent failures.

Table 1: Feature History Table

Feature name	Release information	Feature description
AuditD process keepalive	Cisco IOS XR 26.3.1	AuditD keepalive periodically generates an identifiable Linux audit event at a configurable interval between 10 and 43,200 minutes. Monitoring systems can use these events to verify AuditD health and detect interruptions in audit-event generation or delivery. Additionally, the feature provides automated syslog notifications for service state changes across all nodes. This proactive monitoring eliminates silent failures, ensuring continuous compliance and enhanced operational visibility for large-scale deployments. CLI keywords introduced: The keywords **keepalive** and **interval** are added to the **linux security audit** command.

AuditD process keepalive

Starting with Release 26.3.1, NCS 1020 supports an AuditD keepalive capability. When you enable keepalive, the system periodically generates an identifiable Linux audit event at a user-configurable interval using the **linux security audit keepalive interval** *interval* command. This keepalive event verifies that AuditD process is running and the audit log forwarding remains operational, improving detection of silent failures and strengthening auditability across distributed system fleets.

AuditD process keepalive produces periodic, identifiable Linux audit events that act as heartbeat signals for monitoring systems, helping detect failures in audit-event generation or delivery.

AuditD process keepalive works independently of remote syslog forwarding. If remote syslog forwarding is enabled, NCS 1020 forwards keepalive events to the configured remote syslog server. If remote syslog forwarding is not enabled, NCS 1020 stores the keepalive events in the local audit log.

Each keepalive event is written to the AuditD log as an identifiable record. You can use this record to confirm that:

- AuditD is running
- the audit event path is working
- audit events continue to reach the remote syslog server, if forwarding is enabled

Benefits of AuditD process keepalive

These are key benefits of the AuditD process keepalive:

- Confirms AuditD liveness automatically without manual device checks.
- Helps detect silent AuditD or log-pipeline failures earlier.
- Supports large-scale monitoring across distributed system fleets.
- Improves compliance verification by providing a positive audit signal.
- Allows operators to configure hearbeat log frequency.

Guidelines for AuditD process keepalive

Follow these guidelines when deploying AuditD process keepalive:

- Configure the keepalive interval in minutes. The supported range is 10 to 43200 minutes.
- Filter on the `audit_keepalive` key in your monitoring tools so that you can identify keepalive events separately from operational audit events.
- Use the `location` field in the audit log, when present, to identify the source node for a keepalive event. This field helps you distinguish events from different route processor, line card, sysadmin, or host locations.
- Enable AuditD process keepalive explicitly. The feature is not active until you enable it.

Restrictions for AuditD process keepalive

Always remember these restrictions when deploying AuditD process keepalive:

- AuditD process keepalive verifies AuditD liveness. It does not replace general device health monitoring.
- Keepalive event delivery to a remote server depends on remote syslog forwarding being configured and operational.
- If remote forwarding is not configured, the feature still generates keepalive events, but NCS 1020 stores them locally.
- Verify platform and release availability before deployment.

Configure the AuditD process keepalive

Ensure NCS 1020 AuditD generates keepalive audit events at a configured interval and optionally forwards them to a remote syslog server for monitoring.

Use this task to maintain the integrity of audit logging by confirming periodic keepalive events. You can forward these events to a remote syslog server or store them locally for review.

Before you begin

- Decide how often you want NCS 1020 to generate keepalive events.
- If you want to forward keepalive events to a remote syslog server, configure the remote syslog destination on the system.

Follow these steps to configure AuditD process keepalive:

Procedure

Step 1 Enable AuditD process keepalive and set the interval.

Example:

```
RP/0/RP0/CPU0:ios# linux security audit keepalive interval 1010
```

To disable AuditD process keepalive, use the **no linux security audit keepalive interval 1010** command.

Step 2 Enable audit log forwarding.

Example:

```
RP/0/RP0/CPU0:ios# linux security audit logging syslog
```

Step 3 Configure the remote syslog destination.

Example:

```
RP/0/RP0/CPU0:ios#  logging 10.0.1.2 vrf default port 514
RP/0/RP0/CPU0:ios(config)# commit
```

Step 4 If you enabled remote forwarding, verify the forwarding status.

Example:

```
RP/0/RP0/CPU0:ios#  show linux security audit logging syslog
Mon Aug 10 10:18:01.703 IST
status: disabled
syslog-server(s):
ipaddr: 10.0.1.2 vrf: vrf-default port: 514
```

Step 5 Confirm that keepalive events are generated:

- Check on the remote syslog server if remote forwarding is enabled and the following syslogs are generated.

```
#Audit configuration syslog
<182>1 2026-03-29T12:41:19.653359+05:30 NCS1020_B0_DT_01 SECURITY-AUDIT-6-EVENT - - -
type=CONFIG_CHANGE msg=audit(1774768279.648:2200): auid=4294967295 ses=4294967295
subj=system_u:system_r:auditctl_t:s0 op=add_rule key="audit_keepalive" list=4 res=1#035AUID="unset”


#AuditD keepalive interval syslog
```

```
<182>1 2026-03-29T12:41:29.105188+05:30 NCS1020_B0_DT_01 SECURITY-AUDIT-6-EVENT - - - type=SYSCALL
 msg=audit(1774768289.101:2235): arch=c000003e syscall=87 success=yes exit=0 a0=7fe4a994a60c
a1=7fe4a994a47b a2=1 a3=6 items=2 ppid=8348 pid=13338 auid=4294967295 uid=0 gid=1000 euid=0 suid=0
 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=4294967295 comm="xr_auditd"
exe="/opt/cisco/install-iosxr/base/bin/xr_auditd" subj=system_u:system_r:iosxr_t:s0
key="audit_keepalive"#035ARCH=x86_64 SYSCALL=unlink AUID="unset" UID="root" GID="iosxr" EUID="root"
 SUID="root" FSUID="root" EGID="iosxr" SGID="iosxr" FSGID="iosxr"
```

Note
By default, the syslogs are generated in `/var/log/syslog/`. Otherwise, the syslogs are generated in the path configured on the remote syslog server.

- Check in the local audit log at `/var/log/audit/audit.log` if remote forwarding is not enabled.

NCS 1020 generates periodic keepalive audit events at the configured interval.

What to do next

Configure your monitoring system to alert when expected `audit_keepalive` events stop arriving for a device or location.