

Configure Audit Log Reporting

This chapter describes how to configure audit log reporting on Cisco NX-OS devices.

This chapter contains the following sections:

- AuditD, on page 1
- Guidelines and Limitations, on page 1
- Configure AuditD, on page 2
- Monitor Rules, on page 3
- Verifying AuditD Configuration, on page 4

AuditD

Beginning with Cisco NX-OS Release 10.6(1)F, you can enable AuditD feature to monitor the commands that are executed in guest shell.

Guidelines and Limitations

Following are the guidelines and limitations for AuditD:

- This feature can be enabled only on platforms that have memory of 24GB or more.
- No SNMP Support is available for this feature.
- Tetragon and AuditD features cannot be enabled together. Only one of them can be configured at a time.
- AuditD rules are read-only rules and should not be modified.
- On NX-OS Release10.6(1)F, syslog format for this feature is AUDIT-6-INFO.
- This feature will monitor activities in guest-shell and supervisor only. Monitoring activities on LC or vHost are not supported.
- For audit logs, NX-OS syslog supports maximum syslog size of 1024 bytes (including syslog header). If audit log size exceeds beyond that limit the audit log gets truncated and printed to syslog.
- Beginning with Cisco NX-OS Release 10.6(2)F, these changes are introduced:
    - Syslog format for audit syslog format is AUDIT-6-EVENT.

- Audit log message is rate limited to 1000 message/second. When audit queue size is 1000 messages, any messages generated will get tail dropped by kernel audit.
- In a 4 minute time period, if linux AuditD gets restarted 5 times, it's an error condition and 6th restart within that period is stopped and syslog will be printed:

```
2025 Sep 29 21:29:35 utit_swtele_tb1 %AUDIT-2-AUDITD_EXIT: audit service restarted
more than max restart counts
```

Configure AuditD

Follow the steps to configure AuditD.

Procedure

Step 1 Use the **configure terminal** command to enter global configuration mode.

Step 2 Use the **feature audit** command to enable AuditD.

Use **No** form of this command to disable the feature.

Step 3 Use the **audit monitor {all | authlog-files | cron-files | dns-client-files | docker | guest-shell | kernel-module-mgmt | process-audit | system-log-files | system-login-reboot | system-software | system-time-change | user-group-config-files | user-privilege-mgmt}** command to enable the rules for AuditD including the rules for Guest Shell.

You cannot configure this command if you have already configured **audit monitor guest-shell** . You need to disable **audit monitor guest-shell** before configuring this command. Use **No** form of this command to delete the configuration.

All - Enable all the rules

guest-shell - Monitor commands executed in guest-shell

From NX-OS 10.6(2)F, following options are introduced:

authlog-files – Monitor authentication log files

cron-files – Monitor cron job files

dns-client-files – Monitor dns client files

docker – Monitor docker

kernel-module-mgmt – Monitor kernel module management

process-audit – Monitor process audit

system-log-files – Monitor system log files

system-login-reboot – Monitor system login and reboot

system-software – Monitor system software

system-time-change – Monitor system time change

user-group-config-files – Monitor user group config files

user-privilege-mgmt – Monitor user privilege mgmt

Step 4 Use the **audit monitor guest-shell** command to enable rules to monitor guest-shell commands.

You cannot configure this command if you have already configured **audit monitor all** . You need to disable **audit monitor all** before configuring this command. Use **No** form of this command to delete the configuration.

Step 5 Use the **logging level audit 6** command to enable AuditD logs print to syslog.

By default, this configuration is disabled. Default logging level is 5. To enable syslog printing for AuditD, apply audit 6. This is an existing logging level configuration that helps streaming syslog to remote server. Use **No** form of this command to delete the configuration.

Audit logs will be available on the switch in /nxos/tmp/auditd/audit.log . Maximum of 5 files each of 8MB can be created in /nxos/tmp/auditd/, and after that logs will get rotated. It is recommended to get the AuditD logs pushed to syslog server.

Step 6 Use the **logging logfile messages 6 size 4194304 persistent threshold 0** command to stream syslog.

Set the logging level to 6.

Monitor Rules

- Following are the monitor rules for guest-shell:

```
-a always,exit -F arch=b64 -S execve -F
dir=/isan/vdc_1/virtual-instance/guestshell+/rootfs -F key=gShell_Cmds
-a always,exit -F arch=b32 -S execve -F
dir=/isan/vdc_1/virtual-instance/guestshell+/rootfs -F key=gShell_Cmds
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/crontab -p wa -k
gShell_cron_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/cron.d -p wa -k gShell_cron_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/cron.daily -p wa -k
gShell_cron_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/cron.hourly -p wa -k
gShell_cron_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/cron.weekly -p wa -k
gShell_cron_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/cron.monthly -p wa -k
gShell_cron_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/bin/kmod -p wa -k
gShell_modules_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/passwd -p wa -k
gShell_passwd_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/shadow -p wa -k
gShell_shadow_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/group -p wa -k gShell_group_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/sudoers -p wa -k
gShell_sudoers_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/hosts -p wa -k gShell_hosts_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/etc/resolv.conf -p wa -k
gShell_dns_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/var/volatile/log -p wa -k
gShell_log_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/usr/bin -p wa -k gShell_usr_bin_changes
-w /isan/vdc_1/virtual-instance/guestshell+/rootfs/usr/sbin -p wa -k
gShell_usr_sbin_changes
```

- Following are the monitor rules for supervisor (default):

```
w /etc/crontab -p wa -k cron_changes
-w /etc/cron.d -p wa -k cron_changes
-w /etc/cron.daily -p wa -k cron_changes
-w /etc/cron.hourly -p wa -k cron_changes
-w /etc/cron.weekly -p wa -k cron_changes
-w /etc/cron.monthly -p wa -k cron_changes
-w /bin -p wa -k bin_changes
-w /sbin -p wa -k sbin_changes
-w /usr/bin -p wa -k usr_bin_changes
-w /usr/sbin -p wa -k usr_sbin_changes
-w /usr/bin/dockerd -p wa -k docker_daemon
-w /bin/kmod -p x -k modules_changes
-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_changes
-w /etc/group -p wa -k group_changes
-w /etc/sudoers -p wa -k sudoers_changes
-w /etc/hosts -p wa -k hosts_changes
-w /etc/resolv.conf -p wa -k dns_changes
-w /etc/localtime -p wa -k time_changes
-w /var/volatile/log/auth.log -p wa -k auth_logs
-w /var/volatile/log/sudo.log -p wa -k sudo_usage
-w /var/volatile/log/wtmp -p wa -k shutdown_reboot
-w /var/volatile/log -p wa -k log_changes
-w /logflash/log -p wa -k log_changes
-w /var/lib/docker -p wa -k docker_storage
-a always,exit -F arch=b64 -S execve -F path=/usr/bin/docker -F key=docker_commands
```

Verifying AuditD Configuration

Use the following commands to see various configuration details about AuditD:

Command	Purpose

show audit status	Displays audit status.
	Example output:
	`switch(config)# show audit status`
	`Backlog: 0`
	`Backlog Limit: 64`
	`Backlog Wait Time: 18000`
	`Enabled: 1`
	`Enabled Timestamp: 2025-Aug-08 21:44:35.278358`
	`Failure: 0`
	`Login UID Immutable: 0 unlocked`
	`Lost: 0`
	`PID: 25426`
	`Rate Limit: 1000`
	`Restart Counts: 0`
	`Restart Timestamp:`
	`switch(config)#`

show running-config audit [all]	Displays the current running configuration for the AuditD feature.
show logging level audit	Displays default logging level and current logging level status.
show tech-support audit	Displays the technical support output for AuditD.