監査ログのレポートの設定

この章では、Cisco NX-OS デバイスで監査ログのレポートを設定する方法について説明します。

この章は、次の項で構成されています。

AuditD

Cisco NX-OSリリース 10.6(1)F 以降、AuditD 機能を有効にして、ゲストシェルで実行されるコマンドをモニタリングできます。

注意事項と制約事項

次に、AuditD のガイドラインと制限事項を示します。

- この機能は、16GB を超えるメモリを搭載したプラットフォームでのみ有効にできます。
- この機能では SNMP のサポートを使用できません。
- Tetragon 機能と AuditD 機能を同時に有効にすることはできません。一度に設定できるのは 1 つだけです。
- AuditD ルールは読み取り専用ルールなので、変更できません。
- NX- OS Release 10.6(1)F の場合、この機能の syslog 形式は AUDIT-6-INFO です。
- この機能は、ゲストシェルとスーパーバイザのアクティビティのみをモニタリングします。LC または vHost でのモニタリングアクティビティはサポートされていません。

AuditD 設定

手順に従って、AuditD を設定します。

手順の概要

1. **configure terminal**
2. **feature audit**
3. **audit monitor all**
4. **audit monitor guest-shell**
5. **logging level audit 6**
6. **logging logfile messages 6 size 4194304 persistent threshold 0**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**feature audit**	AuditD機能を有効にします。この機能をディセーブルにするには、このコマンドの **No** 形式を使用します。
ステップ 3	**audit monitor all**	ゲストシェルのルールを含むAuditDのすべてのルールを有効にします。**audit monitor guest-shell**をすでに設定している場合、このコマンドは設定できません。このコマンドを設定する前に、**audit monitor guest-shell** を無効にする必要があります。このコマンドの **No** 形式は、構成を削除します。
ステップ 4	**audit monitor guest-shell**	ゲストシェル コマンドをモニターするルールを有効にします。**audit monitor all**をすでに設定している場合、このコマンドは設定できません。このコマンドを設定する前に、**audit monitor all** を無効にする必要があります。このコマンドの **No** 形式は、構成を削除します。
ステップ 5	**logging level audit 6**	syslog への AuditD ログの出力を有効にします。デフォルトでは、この構成は無効になっています。デフォルトのログレベルは 5 です。AuditD の syslog 出力を有効にするには、audit 6 を適用します。これは、リモートサーバーへのストリーミング syslog に

	コマンドまたはアクション	目的
		役立つ既存のロギング レベルの設定です。このコマンドの **No** 形式は、構成を削除します。 監査ログは、スイッチの /nxos/tmp/auditd/audit.log に保存されます。それぞれ 8MB の最大 5 つのファイルを /nxos/tmp/auditd/ に作成できます。これを超えるとログはローテーションされます。AuditD ログは syslog サーバーにプッシュすることをお勧めします。
ステップ 6	**logging logfile messages 6 size 4194304 persistent threshold 0**	syslog をストリーミングします。ログ レベルを 6 に設定します。

モニター ルール

- ゲストシェルのモニター ルールは次のとおりです。

```
-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
```

- スーパーバイザのモニター ルールは次のとおりです（デフォルト）。

```
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
```

AuditD 設定の確認

AuditD に関するさまざまな設定の詳細を表示するには、次のコマンドを使用します：

コマンド	目的

show audit status	監査ステータスを表示します。
	出力例：
	`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]	AuditD機能の現在の実行コンフィギュレーションを表示します。
show logging level audit	デフォルトのロギングレベルと現在のロギングレベルのステータスを表示します。

コマンド	目的
show tech-support auditd	AuditD のテクニカル サポート出力を表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。