



# Gérer les configurations d'audit

## ONTAP 9

NetApp  
April 24, 2024

# Sommaire

- Gérer les configurations d’audit ..... 1
  - Rotation manuelle des journaux d’événements d’audit ..... 1
  - Activation et désactivation de l’audit sur les SVM ..... 1
  - Affiche des informations sur les configurations d’audit ..... 2
  - Commandes permettant de modifier les configurations d’audit ..... 4
  - Supprimer une configuration d’audit ..... 5
  - Comprenez les implications du rétablissement du cluster ..... 5

# Gérer les configurations d'audit

## Rotation manuelle des journaux d'événements d'audit

Avant de pouvoir afficher les journaux d'événements d'audit, ils doivent être convertis en formats lisibles par l'utilisateur. Si vous souhaitez afficher les journaux des événements d'une machine virtuelle de stockage (SVM) spécifique avant que ONTAP ne fasse automatiquement pivoter le journal, vous pouvez faire tourner manuellement les journaux des événements d'audit sur un SVM.

### Étape

1. Faites pivoter les journaux d'événements d'audit à l'aide de `vserver audit rotate-log` commande.

```
vserver audit rotate-log -vserver vs1
```

Le journal des événements d'audit est enregistré dans le répertoire du journal des événements d'audit SVM au format spécifié par la configuration d'audit (XML ou EVTX), et peut être consulté à l'aide de l'application appropriée.

## Activation et désactivation de l'audit sur les SVM

Vous pouvez activer ou désactiver l'audit sur les serveurs virtuels de stockage (SVM). Vous pouvez désactiver l'audit des fichiers et des répertoires temporairement. Vous pouvez activer l'audit à tout moment (si une configuration d'audit existe).

### Ce dont vous avez besoin

Avant de pouvoir activer l'audit sur le SVM, la configuration d'audit du SVM doit déjà exister.

["Créez la configuration d'audit"](#)

### Description de la tâche

La désactivation de l'audit ne supprime pas la configuration d'audit.

### Étapes

1. Exécutez la commande appropriée :

Si vous voulez que l'audit soit...	Entrez la commande...
Activé	<code>vserver audit enable -vserver vserver_name</code>
Désactivé	<code>vserver audit disable -vserver vserver_name</code>

2. Vérifiez que l'audit est dans l'état souhaité :

```
vserver audit show -vserver vserver_name
```

### Exemples

L'exemple suivant permet l'audit du SVM vs1 :

```
cluster1::> vsserver audit enable -vsserver vs1

cluster1::> vsserver audit show -vsserver vs1

                Vserver: vs1
                Auditing state: true
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 10
```

L'exemple suivant désactive l'audit pour SVM vs1 :

```
cluster1::> vsserver audit disable -vsserver vs1

                Vserver: vs1
                Auditing state: false
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 10
```

## Affiche des informations sur les configurations d'audit

Vous pouvez afficher des informations sur les configurations d'audit. Les informations peuvent vous aider à déterminer si la configuration est celle que vous souhaitez mettre en place pour chaque SVM. Les informations affichées vous permettent également de vérifier si une configuration d'audit est activée.

## Description de la tâche

Vous pouvez afficher des informations détaillées sur les configurations d'audit sur tous les SVM. Vous pouvez également personnaliser les informations affichées dans le résultat en spécifiant des paramètres facultatifs. Si vous ne spécifiez aucun des paramètres facultatifs, les éléments suivants s'affichent :

- Nom du SVM auquel s'applique la configuration d'audit
- État d'audit, qui peut être `true` ou `false`

Si l'état d'audit est `true`, l'audit est activé. Si l'état d'audit est `false`, l'audit est désactivé.

- Catégories d'événements à vérifier
- Format du journal d'audit
- Répertoire cible dans lequel le sous-système d'audit stocke les journaux d'audit consolidés et convertis

## Étape

1. Affiche des informations sur la configuration d'audit à l'aide du `vserver audit show` commande.

Pour plus d'informations sur l'utilisation de la commande, consultez les pages de manuels.

## Exemples

L'exemple suivant affiche un résumé de la configuration d'audit de tous les SVM :

```
cluster1::> vserver audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	file-ops	evtx	/audit_log


L'exemple suivant affiche, sous forme de liste, toutes les informations de configuration d'audit de tous les SVM :

```
cluster1::> vserver audit show -instance

Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evtX
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

## Commandes permettant de modifier les configurations d'audit

Si vous souhaitez modifier un paramètre d'audit, vous pouvez modifier la configuration actuelle à tout moment, notamment modifier le chemin d'accès du journal et le format du journal, modifier les catégories d'événements à auditer, enregistrer automatiquement les fichiers journaux et spécifier le nombre maximal de fichiers journaux à enregistrer.

Les fonctions que vous recherchez...	Utilisez cette commande...
Modifiez le chemin de destination du journal	<code>vserver audit modify</code> avec le <code>-destination</code> paramètre
Modifier la catégorie d'événements à auditer	<div> <div></div> <div> <p>Pour auditer les événements de transfert des règles d'accès central, l'option du serveur SMB Dynamic Access Control (DAC) doit être activée sur le serveur SVM (Storage Virtual machine).</p> </div> </div>
Modifiez le format du journal	<code>vserver audit modify</code> avec le <code>-format</code> paramètre
Activation des sauvegardes automatiques en fonction de la taille du fichier journal interne	<code>vserver audit modify</code> avec le <code>-rotate-size</code> paramètre

Activation des sauvegardes automatiques en fonction d'un intervalle de temps	<code>vserver audit modify</code> avec le <code>-rotate</code> <code>-schedule-month</code> , <code>-rotate-schedule</code> <code>-dayofweek</code> , <code>-rotate-schedule-day</code> , <code>-rotate</code> <code>-schedule-hour</code> , et <code>-rotate-schedule-minute</code> paramètres
Spécification du nombre maximal de fichiers journaux enregistrés	<code>vserver audit modify</code> avec le <code>-rotate-limit</code> paramètre

## Supprimer une configuration d'audit

Vous ne souhaitez plus auditer les événements de fichier et de répertoire sur la machine virtuelle de stockage (SVM) et ne souhaitez pas conserver une configuration d'audit sur la SVM, vous pouvez supprimer la configuration d'audit.

### Étapes

1. Désactivez la configuration d'audit :

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Supprimer la configuration d'audit :

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

## Comprenez les implications du rétablissement du cluster

Si vous prévoyez de restaurer le cluster, sachez que le processus de restauration suivi par la ONTAP est exécuté lors de l'audit de serveurs virtuels de stockage (SVM) dans le cluster. Vous devez effectuer certaines actions avant de revenir en retour.

### Restauration vers une version d'ONTAP qui ne prend pas en charge l'audit des événements de connexion et de déconnexion SMB et des événements de mise en attente des règles d'accès central

La prise en charge de l'audit des événements de connexion et de déconnexion SMB et de l'activation des règles d'accès central commence avec clustered Data ONTAP 8.3. Si vous rétablissez une version de ONTAP qui ne prend pas en charge ces types d'événements et que vous disposez de configurations d'audit qui surveillent ces types d'événements, vous devez modifier la configuration d'audit de ces SVM activés par audit avant de procéder à un rétablissement. Vous devez modifier la configuration de manière à ce que seuls les événements file-op soient audités.

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.