Créer une configuration d'audit de fichier et de répertoire sur les SVM

ONTAP 9

NetApp
April 24, 2024

Sommaire

Créer une configuration d'audit de fichier et de répertoire sur les SVM

Créez la configuration d'audit

La création d'une configuration d'audit de fichier et de répertoire sur votre SVM (Storage Virtual machine) comprend les options de configuration disponibles, la planification de la configuration, puis la configuration et l'activation de la configuration. Vous pouvez ensuite afficher des informations sur la configuration d'audit pour confirmer que la configuration résultante est la configuration souhaitée.

Avant de pouvoir commencer l'audit des événements de fichiers et de répertoires, vous devez créer une configuration d'audit sur la machine virtuelle de stockage (SVM).

Avant de commencer

Si vous prévoyez de créer une configuration d'audit pour la mise en attente des règles d'accès central, un serveur SMB doit exister sur le SVM.

- Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, les événements de staging de stratégie d'accès central ne sont générés que si le contrôle d'accès dynamique est activé.

  Le contrôle d'accès dynamique est activé par le biais d'une option de serveur SMB. Elle n'est pas activée par défaut.

- Si les arguments d'un champ d'une commande ne sont pas valides, par exemple des entrées non valides pour les champs, des entrées dupliquées et des entrées non existantes, la commande échoue avant la phase d'audit.

  Ces échecs ne génèrent pas d'enregistrement d'audit.

Description de la tâche

Si le SVM est une source de reprise d'activité du SVM, le chemin de destination ne peut pas se trouver sur le volume root.

Étape

1. À l'aide des informations de la fiche de planification, créez la configuration d'audit pour faire pivoter les journaux d'audit en fonction de la taille du journal ou d'une planification :

Si vous souhaitez faire pivoter les journaux d'audit en…	Entrer…
Taille du journal	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change

user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
Un planning	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Exemples

L'exemple suivant crée une configuration d'audit qui vérifie les opérations de fichiers et les événements de connexion et de déconnexion SMB (par défaut) à l'aide de la rotation basée sur la taille. Le format du journal est `EVTX` (valeur par défaut). Les journaux sont stockés dans le `/audit_log` répertoire. La taille limite du fichier journal est de `200 MB`. Les journaux pivotent lorsqu'ils atteignent 200 Mo de taille :

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

L'exemple suivant crée une configuration d'audit qui vérifie les opérations de fichiers et les événements de connexion et de déconnexion SMB (par défaut) à l'aide de la rotation basée sur la taille. Le format du journal est `EVTX` (valeur par défaut). Les journaux sont stockés dans le `/cifs_event_logs` répertoire. La taille limite du fichier journal est de `100 MB` (valeur par défaut) et la limite de rotation du journal est `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

L'exemple suivant crée une configuration d'audit qui audite les opérations de fichiers, les événements de connexion et de déconnexion CIFS, ainsi que les événements d'activation de stratégie d'accès central à l'aide d'une rotation basée sur le temps. Le format du journal est `EVTX` (valeur par défaut). Les journaux d'audit sont pivotés tous les mois, à 12:30 tous les jours de la semaine. La limite de rotation du log est de `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Activation de l'audit sur le SVM

Une fois la configuration d'audit terminée, vous devez activer l'audit sur la machine virtuelle de stockage (SVM).

Ce dont vous avez besoin

La configuration d'audit SVM doit déjà exister.

Description de la tâche

Lorsqu'une configuration SVM Disaster Recovery ID rebuter est démarrée en premier (une fois l'initialisation de SnapMirror terminée) et que le SVM dispose d'une configuration d'audit, ONTAP désactive automatiquement la configuration d'audit. L'audit est désactivé sur le SVM en lecture seule pour empêcher le remplissage des volumes de transit. Vous pouvez activer l'audit uniquement après la rupture de la relation SnapMirror et la SVM est read-write.

Étape

1. Activer l'audit sur le SVM :

   ```
   vserver audit enable -vserver vserver_name
   ```

   ```
   vserver audit enable -vserver vs1
   ```

Vérifiez la configuration de l'audit

Une fois la configuration d'audit terminée, vous devez vérifier que l'audit est correctement configuré et activé.

Étapes

1. Vérifiez la configuration de l'audit :

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

   La commande suivante s'affiche sous forme de liste toutes les informations de configuration d'audit pour la machine virtuelle de stockage (SVM) vs1 :

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                                Vserver: vs1
                       Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                            Log Format: evtx
                  Log File Size Limit: 200MB
        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
   ```