Gérer les configurations d'audit

ONTAP 9

NetApp
April 24, 2024

Sommaire

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	`vserver audit enable -vserver vserver_name`
Désactivé	`vserver audit disable -vserver vserver_name`

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::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver 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::> vserver audit disable -vserver 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	`vserver audit modify` avec le `-destination` paramètre
Modifier la catégorie d'événements à auditer	`vserver audit modify` avec le `-events` paramètre 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).
Modifiez le format du journal	`vserver audit modify` avec le `-format` paramètre
Activation des sauvegardes automatiques en fonction de la taille du fichier journal interne	`vserver audit modify` avec le `-rotate-size` paramètre

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