Exécuter des traces de sécurité

ONTAP 9

NetApp
April 24, 2024

Sommaire

Exécuter des traces de sécurité

Présenter les traces de sécurité

Une trace de sécurité implique la création d'un filtre de trace de sécurité, la vérification des critères de filtre, la génération de demandes d'accès sur un client SMB ou NFS qui correspondent aux critères de filtre, ainsi que l'affichage des résultats.

Une fois que vous avez terminé d'utiliser un filtre de sécurité pour capturer des informations de trace, vous pouvez modifier le filtre et le réutiliser ou le désactiver si vous n'en avez plus besoin. Après avoir affiché et analysé les résultats de trace du filtre, vous pouvez les supprimer s'ils ne sont plus nécessaires.

Créer des filtres de trace de sécurité

Vous pouvez créer des filtres de trace de sécurité qui détectent les opérations des clients SMB et NFS sur les SVM (Storage Virtual machines) et vérifient tous les contrôles d'accès correspondant au filtre. Vous pouvez utiliser les résultats des tracés de sécurité pour valider votre configuration ou résoudre des problèmes d'accès.

Description de la tâche

Il existe deux paramètres requis pour la commande vserver Security trace filter create :

Paramètres requis	Description
`-vserver vserver_name`	*Nom du SVM* Nom du SVM qui contient les fichiers ou les dossiers sur lesquels vous souhaitez appliquer le filtre de trace de sécurité.
`-index index_number`	*Filtrer l'index numéro* Le numéro d'index que vous souhaitez appliquer au filtre. Vous êtes limité à un maximum de 10 filtres de trace par SVM. Les valeurs autorisées pour ce paramètre sont de 1 à 10.

Un certain nombre de paramètres de filtre facultatifs vous permettent de personnaliser le filtre de trace de sécurité afin de réduire les résultats générés par le tracé de sécurité :

Paramètre de filtre	Description
`-client-ip IP_Address`	Ce filtre spécifie l'adresse IP à partir de laquelle l'utilisateur accède au SVM.

`-path path`	Ce filtre indique le chemin d'accès sur lequel appliquer le filtre de suivi des autorisations. La valeur pour `-path` peut utiliser l'un des formats suivants : • Le chemin complet, en commençant par la racine du partage ou de l'exportation • Chemin partiel, relatif à la racine du partage Vous devez utiliser les séparateurs de répertoire de style UNIX du répertoire de style NFS dans la valeur de chemin d'accès.
`-windows-name win_user_name` ou `-unix -name``unix_user_name`	Vous pouvez spécifier le nom d'utilisateur Windows ou le nom d'utilisateur UNIX dont vous souhaitez effectuer le suivi des demandes d'accès. La variable de nom d'utilisateur n'est pas sensible à la casse. Vous ne pouvez pas spécifier à la fois un nom d'utilisateur Windows et un nom d'utilisateur UNIX dans le même filtre. Même si vous pouvez suivre les événements d'accès SMB et NFS, il est possible d'utiliser l'utilisateur UNIX mappé et les groupes d'utilisateurs UNIX mappés lors des vérifications d'accès sur des données de style de sécurité UNIX ou mixtes.
`-trace-allow` {`yes`	`no`}
Le suivi des événements de refus est toujours activé pour un filtre de trace de sécurité. Vous pouvez éventuellement suivre les événements. Pour suivre les événements d'autorisation, définissez ce paramètre sur `yes`.	`-enabled` {`enabled`
`disabled`}	Vous pouvez activer ou désactiver le filtre de trace de sécurité. Par défaut, le filtre de trace de sécurité est activé.
`-time-enabled integer`	Vous pouvez spécifier un délai d'attente pour le filtre, après lequel il est désactivé.

Étapes

1. Créer un filtre de trace de sécurité :

   ```
   vserver security trace filter create -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   `filter_parameters` est une liste des paramètres de filtre facultatifs.

   Pour plus d'informations, consultez les pages de manuels relatives à la commande.

2. Vérifiez l'entrée du filtre de trace de sécurité :

```
vserver security trace filter show -vserver vserver_name -index index_number
```

Exemples

La commande suivante crée un filtre de trace de sécurité pour tout utilisateur accédant à un fichier avec un chemin de partage `\\server\share1\dir1\dir2\file.txt` À partir de l'adresse IP 10.10.10.7. Le filtre utilise un chemin complet pour le `-path` option. L'adresse IP du client utilisée pour accéder aux données est 10.10.10.7. Le filtre est sorti après 30 minutes :

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

La commande suivante crée un filtre de trace de sécurité utilisant un chemin relatif pour l' `-path` option. Le filtre trace l'accès pour un utilisateur Windows nommé « joe ». Joe accède à un fichier avec un chemin de partage `\\server\share1\dir1\dir2\file.txt`. Les traces de filtre autorisent et refusent les événements :

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                Vserver: vs1
                           Filter Index: 2
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: mydomain\joe
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
                 Minutes Filter is Enabled: 60
```

Affiche des informations sur les filtres de trace de sécurité

Vous pouvez afficher des informations sur les filtres de trace de sécurité configurés sur votre SVM (Storage Virtual machine). Cela vous permet de voir quels types d'événements d'accès chaque filtre trace.

Étape

1. Affiche des informations sur les entrées du filtre de trace de sécurité à l'aide de `vserver security trace filter show` commande.

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

Exemples

La commande suivante affiche des informations sur tous les filtres de trace de sécurité sur le SVM vs1 :

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Affiche les résultats du suivi de sécurité

Vous pouvez afficher les résultats de suivi de sécurité générés pour les opérations de fichiers qui correspondent aux filtres de trace de sécurité. Les résultats permettent de valider votre configuration de sécurité d'accès aux fichiers ou de résoudre les problèmes d'accès aux fichiers SMB et NFS.

Ce dont vous avez besoin

Un filtre de trace de sécurité activé doit exister et des opérations doivent avoir été effectuées à partir d'un client SMB ou NFS correspondant au filtre de trace de sécurité pour générer les résultats de trace de sécurité.

Description de la tâche

Vous pouvez afficher un récapitulatif de tous les résultats de la trace de sécurité ou personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque les résultats du suivi de sécurité contiennent un grand nombre d'enregistrements.

Si vous ne spécifiez aucun des paramètres facultatifs, les éléments suivants s'affichent :

- Nom de la machine virtuelle de stockage (SVM)
- Nom du nœud
- Numéro d'index de trace de sécurité
- Style de sécurité
- Chemin
- Raison
- Nom d'utilisateur

  Le nom d'utilisateur s'affiche en fonction de la configuration du filtre de trace :

Si le filtre est configuré…	Alors…
Avec un nom d'utilisateur UNIX	Le résultat du suivi de sécurité affiche le nom d'utilisateur UNIX.
Avec un nom d'utilisateur Windows	Le résultat du suivi de sécurité affiche le nom d'utilisateur Windows.
Sans nom d'utilisateur	Le résultat du suivi de sécurité affiche le nom d'utilisateur Windows.

Vous pouvez personnaliser la sortie à l'aide de paramètres facultatifs. Voici certains des paramètres facultatifs que vous pouvez utiliser pour affiner les résultats renvoyés dans le résultat de la commande :

Paramètre facultatif	Description
`-fields field_name, ...`	Affiche la sortie sur les champs que vous choisissez. Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.
`-instance`	Affiche des informations détaillées sur les événements de trace de sécurité. Utilisez ce paramètre avec d'autres paramètres facultatifs pour afficher des informations détaillées sur des résultats de filtre spécifiques.
`-node node_name`	Affiche des informations uniquement sur les événements du nœud spécifié.
`-vserver vserver_name`	Affiche des informations uniquement sur les événements du SVM spécifié.
`-index integer`	Affiche des informations sur les événements survenus à la suite du filtre correspondant au numéro d'index spécifié.
`-client-ip IP_address`	Affiche des informations sur les événements survenus à la suite de l'accès au fichier à partir de l'adresse IP du client spécifiée.
`-path path`	Affiche des informations sur les événements qui se sont produits suite à l'accès au fichier au chemin spécifié.
`-user-name user_name`	Affiche des informations sur les événements qui se sont produits à la suite de l'accès au fichier par l'utilisateur Windows ou UNIX spécifié.
`-security-style security_style`	Affiche des informations sur les événements survenus sur les systèmes de fichiers avec le style de sécurité spécifié.

Pour plus d'informations sur les autres paramètres facultatifs que vous pouvez utiliser avec la commande, reportez-vous à la page man.

Étape

1. Affiche les résultats du filtre de trace de sécurité à l'aide de l' `vserver security trace trace-result show` commande.

   `vserver security trace trace-result show -user-name domain\user`

   ```
   Vserver: vs1

   Node     Index   Filter Details         Reason
   -------- ------- ---------------------  ----------------------------
   node1    3       User:domain\user       Access denied by explicit ACE
                    Security Style:mixed
                    Path:/dir1/dir2/

   node1    5       User:domain\user       Access denied by explicit ACE
                    Security Style:unix
                    Path:/dir1/
   ```

Modifier les filtres de trace de sécurité

Si vous souhaitez modifier les paramètres de filtre facultatifs utilisés pour déterminer les événements d'accès qui sont tracés, vous pouvez modifier les filtres de trace de sécurité existants.

Description de la tâche

Vous devez identifier le filtre de trace de sécurité à modifier en précisant le nom de la machine virtuelle de stockage (SVM) sur laquelle le filtre est appliqué et le numéro d'index du filtre. Vous pouvez modifier tous les paramètres de filtre facultatifs.

Étapes

1. Modifier un filtre de trace de sécurité :

   `vserver security trace filter modify -vserver vserver_name -index index_numberfilter_parameters`

   - `vserver_name` Est le nom du SVM sur lequel vous souhaitez appliquer un filtre de trace de sécurité.
   - `index_number` est le numéro d'index que vous souhaitez appliquer au filtre. Les valeurs autorisées pour ce paramètre sont de 1 à 10.
   - `filter_parameters` est une liste des paramètres de filtre facultatifs.

2. Vérifiez l'entrée du filtre de trace de sécurité :

   `vserver security trace filter show -vserver vserver_name -index index_number`

Exemple

La commande suivante modifie le filtre de trace de sécurité avec l'index numéro 1. Le filtre trace les

événements pour tout utilisateur accédant à un fichier avec un chemin de partage `\\server\share1\dir1\dir2\file.txt` À partir de n'importe quelle adresse IP. Le filtre utilise un chemin complet pour le `-path` option. Les traces de filtre autorisent et refusent les événements :

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                 Vserver: vs1
                            Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Supprimer les filtres de trace de sécurité

Lorsque vous n'avez plus besoin d'une entrée de filtre de trace de sécurité, vous pouvez la supprimer. Étant donné que vous pouvez disposer d'un maximum de 10 filtres de suivi de sécurité par machine virtuelle de stockage (SVM), la suppression des filtres inutiles vous permet de créer de nouveaux filtres si vous avez atteint le maximum.

Description de la tâche

Pour identifier de manière unique le filtre de trace de sécurité que vous souhaitez supprimer, vous devez spécifier les éléments suivants :

- Nom du SVM auquel le filtre de trace est appliqué
- Numéro d'index du filtre de trace

Étapes

1. Identifiez le numéro d'index de filtre de l'entrée de filtre de trace de sécurité que vous souhaitez supprimer :

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

```
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

2. À l'aide des informations de numéro d'index de filtre de l'étape précédente, supprimez l'entrée de filtre :

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

   ```
   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. Vérifiez que l'entrée du filtre de trace de sécurité est supprimée :

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

Supprimer les enregistrements de trace de sécurité

Une fois que vous avez terminé d'utiliser un enregistrement de suivi de filtre pour vérifier la sécurité d'accès aux fichiers ou pour résoudre les problèmes d'accès client SMB ou NFS, vous pouvez supprimer l'enregistrement de trace de sécurité du journal de suivi de sécurité.

Description de la tâche

Avant de pouvoir supprimer un enregistrement de trace de sécurité, vous devez connaître le numéro de séquence de l'enregistrement.

> Chaque machine virtuelle de stockage (SVM) peut stocker un maximum de 128 traces. Si le maximum est atteint sur la SVM, les anciens enregistrements de trace sont automatiquement supprimés au fur et à mesure de l'ajout de nouveaux enregistrements. Si vous ne souhaitez pas supprimer manuellement les enregistrements de trace sur ce SVM, vous pouvez laisser ONTAP supprimer automatiquement les plus anciens résultats de trace une fois que le maximum est atteint pour laisser place à de nouveaux résultats.

Étapes

1. Identifiez le numéro de séquence de l'enregistrement à supprimer :

   ```
   vserver security trace trace-result show -vserver vserver_name -instance
   ```

2. Supprimer l'enregistrement de trace de sécurité :

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name -seqnum integer
   ```

   ```
   vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
   999
   ```

   - `-node node_name` est le nom du nœud de cluster sur lequel l'événement de suivi des autorisations que vous souhaitez supprimer s'est produit.

     Ce paramètre est obligatoire.

   - `-vserver vserver_name` Est le nom du SVM sur lequel l'événement de suivi des permissions que vous souhaitez supprimer s'est produit.

     Ce paramètre est obligatoire.

   - `-seqnum integer` est le numéro de séquence de l'événement de journal que vous souhaitez supprimer.

     Ce paramètre est obligatoire.

Supprimer tous les enregistrements de trace de sécurité

Si vous ne souhaitez pas conserver les enregistrements de trace de sécurité existants, vous pouvez supprimer tous les enregistrements d'un nœud à l'aide d'une seule commande.

Étape

1. Supprimer tous les enregistrements de trace de sécurité :

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name *
   ```

   - `-node node_name` est le nom du nœud de cluster sur lequel l'événement de suivi des autorisations que vous souhaitez supprimer s'est produit.
   - `-vserver vserver_name` Est le nom de la machine virtuelle de stockage (SVM) sur laquelle l'événement de suivi des permissions que vous souhaitez supprimer s'est produit.