Eseguire le tracce di sicurezza

ONTAP 9

NetApp
April 24, 2024

Sommario

Eseguire le tracce di sicurezza

Eseguire una panoramica delle tracce di sicurezza

L'esecuzione di una traccia di protezione implica la creazione di un filtro di traccia di protezione, la verifica dei criteri di filtro, la generazione di richieste di accesso su un client SMB o NFS che corrispondono ai criteri di filtro e la visualizzazione dei risultati.

Dopo aver utilizzato un filtro di sicurezza per acquisire le informazioni di traccia, è possibile modificare il filtro e riutilizzarlo oppure disattivarlo se non è più necessario. Dopo aver visualizzato e analizzato i risultati della traccia del filtro, è possibile eliminarli se non sono più necessari.

Creare filtri di traccia per la sicurezza

È possibile creare filtri di traccia per la sicurezza che rilevano le operazioni dei client SMB e NFS sulle macchine virtuali di storage (SVM) e tracciano tutti i controlli di accesso corrispondenti al filtro. È possibile utilizzare i risultati delle tracce di protezione per convalidare la configurazione o risolvere i problemi di accesso.

A proposito di questa attività

Sono necessari due parametri per il comando vserver Security trace filter create:

Parametri richiesti	Descrizione
`-vserver vserver_name`	*Nome SVM* Il nome della SVM che contiene i file o le cartelle su cui si desidera applicare il filtro di traccia di protezione.
`-index index_number`	*Numero indice del filtro* Il numero di indice che si desidera applicare al filtro. È possibile utilizzare un massimo di 10 filtri di traccia per SVM. I valori consentiti per questo parametro sono compresi tra 1 e 10.

Una serie di parametri di filtro opzionali consente di personalizzare il filtro di traccia di protezione in modo da restringere i risultati prodotti dalla traccia di protezione:

Parametro del filtro	Descrizione
`-client-ip IP_Address`	Questo filtro specifica l'indirizzo IP da cui l'utente accede a SVM.

`-path` `path`	Questo filtro specifica il percorso su cui applicare il filtro di traccia delle autorizzazioni. Il valore per `-path` può utilizzare uno dei seguenti formati: • Il percorso completo, a partire dalla directory principale della condivisione o dell'esportazione • Un percorso parziale, relativo alla radice della condivisione È necessario utilizzare i separatori di directory in stile UNIX di NFS nel valore del percorso.
`-windows-name` `win_user_name` oppure `-unix -name``unix_user_name`	È possibile specificare il nome utente Windows o UNIX di cui si desidera tenere traccia delle richieste di accesso. La variabile del nome utente non fa distinzione tra maiuscole e minuscole. Non è possibile specificare un nome utente Windows e un nome utente UNIX nello stesso filtro. Anche se è possibile tracciare gli eventi di accesso SMB e NFS, l'utente UNIX mappato e i gruppi di utenti UNIX mappati potrebbero essere utilizzati quando si eseguono controlli di accesso su dati misti o UNIX di tipo di sicurezza.
`-trace-allow` {`yes`	`no`}
La funzione di traccia per gli eventi di negazione è sempre abilitata per un filtro di traccia di protezione. Facoltativamente, è possibile tracciare gli eventi Allow. Per tracciare gli eventi Allow, impostare questo parametro su `yes`.	`-enabled` {`enabled`
`disabled`}	È possibile attivare o disattivare il filtro di traccia di protezione. Per impostazione predefinita, il filtro di traccia di protezione è attivato.
`-time-enabled` `integer`	È possibile specificare un timeout per il filtro, dopo il quale viene disattivato.

Fasi

1. Creazione di un filtro di traccia per la protezione:

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

   `filter_parameters` è un elenco di parametri di filtro opzionali.

   Per ulteriori informazioni, vedere le pagine man del comando.

2. Verificare la voce Security trace filter:

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

Esempi

Il comando seguente crea un filtro di traccia di protezione per qualsiasi utente che accede a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt` Dall'indirizzo IP 10.10.10.7. Il filtro utilizza un percorso completo per `-path` opzione. L'indirizzo IP del client utilizzato per accedere ai dati è 10.10.10.7. Il filtro si esaurisce dopo 30 minuti:

```
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       -
```

Il comando seguente crea un filtro di traccia di protezione utilizzando un percorso relativo per `-path` opzione. Il filtro traccia l'accesso di un utente Windows chiamato "joe". Joe sta accedendo a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt`. Le tracce del filtro consentono e negano gli eventi:

```
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
```

Visualizza informazioni sui filtri di traccia per la sicurezza

È possibile visualizzare informazioni sui filtri di traccia di protezione configurati sulla macchina virtuale di storage (SVM). In questo modo è possibile visualizzare i tipi di eventi di accesso che ciascun filtro traccia.

Fase

1. Visualizzare le informazioni relative alle voci del filtro di traccia di protezione utilizzando `vserver`

`security trace filter show` comando.

Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

Esempi

Il seguente comando visualizza informazioni su tutti i filtri di traccia di sicurezza su 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
```

Visualizzare i risultati della traccia di sicurezza

È possibile visualizzare i risultati della traccia di protezione generati per le operazioni dei file che corrispondono ai filtri di traccia di protezione. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza per l'accesso ai file o per risolvere i problemi di accesso ai file SMB e NFS.

Di cosa hai bisogno

Per generare i risultati della traccia di protezione, è necessario che esista un filtro di traccia di protezione abilitato e che siano state eseguite operazioni da un client SMB o NFS che corrisponda al filtro di traccia di protezione.

A proposito di questa attività

È possibile visualizzare un riepilogo di tutti i risultati della traccia di protezione oppure personalizzare le informazioni visualizzate nell'output specificando parametri opzionali. Ciò può essere utile quando i risultati della traccia di protezione contengono un gran numero di record.

Se non si specifica alcun parametro opzionale, viene visualizzato quanto segue:

- Nome SVM (Storage Virtual Machine)
- Nome del nodo
- Numero di indice della traccia di sicurezza
- Stile di sicurezza
- Percorso
- Motivo
- Nome utente

  Il nome utente viene visualizzato in base alla configurazione del filtro di traccia:

Se il filtro è configurato…	Quindi…

Con un nome utente UNIX	Il risultato della traccia di protezione visualizza il nome utente UNIX.
Con un nome utente Windows	Il risultato della traccia di protezione visualizza il nome utente di Windows.
Senza nome utente	Il risultato della traccia di protezione visualizza il nome utente di Windows.

È possibile personalizzare l'output utilizzando parametri opzionali. Alcuni dei parametri facoltativi che è possibile utilizzare per limitare i risultati restituiti nell'output del comando includono:

Parametro facoltativo	Descrizione
`-fields field_name, ...`	Visualizza l'output nei campi scelti. È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.
`-instance`	Visualizza informazioni dettagliate sugli eventi di analisi della sicurezza. Utilizzare questo parametro con altri parametri opzionali per visualizzare informazioni dettagliate sui risultati specifici del filtro.
`-node node_name`	Visualizza solo informazioni sugli eventi nel nodo specificato.
`-vserver vserver_name`	Visualizza solo le informazioni sugli eventi sulla SVM specificata.
`-index integer`	Visualizza le informazioni sugli eventi che si sono verificati come risultato del filtro corrispondente al numero di indice specificato.
`-client-ip IP_address`	Visualizza informazioni sugli eventi che si sono verificati in seguito all'accesso al file dall'indirizzo IP del client specificato.
`-path path`	Visualizza le informazioni sugli eventi che si sono verificati in seguito all'accesso al file al percorso specificato.
`-user-name user_name`	Visualizza informazioni sugli eventi che si sono verificati in seguito all'accesso al file da parte dell'utente Windows o UNIX specificato.
`-security-style security_style`	Visualizza informazioni sugli eventi che si sono verificati nei file system con lo stile di sicurezza specificato.

Consultare la pagina man per informazioni sugli altri parametri opzionali che è possibile utilizzare con il comando.

Fase

1. Visualizzare i risultati del filtro di traccia di protezione utilizzando `vserver security trace trace-result show` comando.

```
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/
```

Modificare i filtri di traccia di protezione

Se si desidera modificare i parametri di filtro opzionali utilizzati per determinare gli eventi di accesso da tracciare, è possibile modificare i filtri di traccia di protezione esistenti.

A proposito di questa attività

È necessario identificare il filtro di traccia di protezione che si desidera modificare specificando il nome della macchina virtuale di storage (SVM) a cui è applicato il filtro e il numero di indice del filtro. È possibile modificare tutti i parametri del filtro opzionali.

Fasi

1. Modificare un filtro di traccia di protezione:

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

   - `vserver_name` È il nome della SVM su cui si desidera applicare un filtro di traccia di protezione.
   - `index_number` è il numero di indice che si desidera applicare al filtro. I valori consentiti per questo parametro sono compresi tra 1 e 10.
   - `filter_parameters` è un elenco di parametri di filtro opzionali.

2. Verificare la voce Security trace filter:

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

Esempio

Il comando seguente modifica il filtro di traccia di protezione con il numero di indice 1. Il filtro traccia gli eventi di qualsiasi utente che accede a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt` Da qualsiasi indirizzo IP. Il filtro utilizza un percorso completo per `-path` opzione. Le tracce del filtro consentono e negano gli eventi:

```
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
```

Eliminare i filtri di traccia di sicurezza

Quando non è più necessario un filtro di traccia di protezione, è possibile eliminarlo. Poiché è possibile disporre di un massimo di 10 filtri di traccia di sicurezza per macchina virtuale di storage (SVM), l'eliminazione dei filtri non necessari consente di creare nuovi filtri se si è raggiunto il massimo.

A proposito di questa attività

Per identificare in modo univoco il filtro di traccia di protezione che si desidera eliminare, è necessario specificare quanto segue:

- Il nome della SVM a cui viene applicato il filtro di traccia
- Il numero dell'indice del filtro di traccia

Fasi

1. Identificare il numero di indice del filtro della voce di Security trace filter che si desidera eliminare:

   ```
   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. Utilizzando le informazioni sul numero di indice del filtro del passaggio precedente, eliminare la voce del filtro:

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

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

3. Verificare che la voce Security trace filter sia stata eliminata:

```
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
```

Eliminare i record di traccia di sicurezza

Dopo aver utilizzato un record di traccia del filtro per verificare la sicurezza dell'accesso ai file o per risolvere i problemi di accesso al client SMB o NFS, è possibile eliminare il record di traccia della protezione dal registro di traccia della protezione.

A proposito di questa attività

Prima di eliminare un record di traccia di protezione, è necessario conoscere il numero di sequenza del record.

> Ogni macchina virtuale di storage (SVM) può memorizzare un massimo di 128 record di traccia. Se si raggiunge il valore massimo sulla SVM, i record di traccia meno recenti vengono eliminati automaticamente quando vengono aggiunti nuovi record. Se non si desidera eliminare manualmente i record di traccia su questa SVM, è possibile consentire a ONTAP di eliminare automaticamente i risultati di traccia meno recenti una volta raggiunto il numero massimo di risultati per creare spazio per i nuovi risultati.

Fasi

1. Identificare il numero di sequenza del record che si desidera eliminare:

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

2. Eliminare il record di traccia di protezione:

```
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` è il nome del nodo del cluster in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

Questo è un parametro obbligatorio.

- `-vserver vserver_name` È il nome della SVM in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

  Questo è un parametro obbligatorio.

- `-seqnum integer` è il numero di sequenza dell'evento di log che si desidera eliminare.

  Questo è un parametro obbligatorio.

Eliminare tutti i record di traccia di sicurezza

Se non si desidera conservare alcun record di traccia di protezione esistente, è possibile eliminare tutti i record di un nodo con un singolo comando.

Fase

1. Eliminare tutti i record di traccia di sicurezza:

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

   - `-node node_name` è il nome del nodo del cluster in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.
   - `-vserver vserver_name` È il nome della macchina virtuale di storage (SVM) su cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.