Execute rastreamentos de segurança

ONTAP 9

NetApp
January 17, 2025

Índice

Execute rastreamentos de segurança

Execute uma visão geral dos rastreamentos de segurança

A execução de um rastreamento de segurança envolve a criação de um filtro de rastreamento de segurança, a verificação dos critérios de filtro, a geração de solicitações de acesso em um cliente SMB ou NFS que correspondam aos critérios de filtro e a visualização dos resultados.

Depois de terminar de usar um filtro de segurança para capturar informações de rastreamento, você pode modificar o filtro e reutilizá-lo ou desativá-lo se não precisar mais dele. Depois de visualizar e analisar os resultados do rastreamento do filtro, você pode excluí-los se eles não forem mais necessários.

Crie filtros de rastreamento de segurança

Você pode criar filtros de rastreamento de segurança que detetam operações de clientes SMB e NFS em máquinas virtuais de armazenamento (SVMs) e rastrear todas as verificações de acesso correspondentes ao filtro. Você pode usar os resultados de rastreamentos de segurança para validar sua configuração ou para solucionar problemas de acesso.

Sobre esta tarefa

Existem dois parâmetros necessários para o comando criar filtro de rastreamento de segurança vserver:

Parâmetros necessários	Descrição
`-vserver vserver_name`	*Nome da SVM* O nome do SVM que contém os arquivos ou pastas em que você deseja aplicar o filtro de rastreamento de segurança.
`-index index_number`	*Número do índice do filtro* O número de índice que você deseja aplicar ao filtro. Você está limitado a um máximo de 10 filtros de rastreamento por SVM. Os valores permitidos para este parâmetro são de 1 a 10.

Vários parâmetros de filtro opcionais permitem personalizar o filtro de rastreamento de segurança para que você possa reduzir os resultados produzidos pelo rastreamento de segurança:

Parâmetro do filtro	Descrição
`-client-ip IP_Address`	Esse filtro especifica o endereço IP a partir do qual o usuário está acessando o SVM.

`-path path`	Este filtro especifica o caminho no qual aplicar o filtro de rastreamento de permissões. O valor para `-path` pode utilizar um dos seguintes formatos: • O caminho completo, a partir da raiz do compartilhamento ou exportação • Um caminho parcial, relativo à raiz do compartilhamento Você deve usar separadores de diretório estilo NFS no valor do caminho.
`-windows-name win_user_name` ou `-unix -name`` `unix_user_name`	Você pode especificar o nome de usuário do Windows ou o nome de usuário UNIX cujas solicitações de acesso você deseja rastrear. A variável de nome de usuário é insensível a maiúsculas e minúsculas. Não é possível especificar um nome de usuário do Windows e um nome de usuário UNIX no mesmo filtro. Mesmo que você possa rastrear eventos de acesso SMB e NFS, o usuário UNIX mapeado e os grupos de usuários UNIX mapeados podem ser usados ao executar verificações de acesso em dados de estilo de segurança misto ou UNIX.
`-trace-allow {yes`	`no`Selecione
O rastreamento para eventos de negação é sempre ativado para um filtro de rastreamento de segurança. Opcionalmente, você pode rastrear eventos de permissão. Para rastrear eventos de permissão, defina este parâmetro como `yes`.	`-enabled {enabled`
`disabled`Selecione	Pode ativar ou desativar o filtro de rastreio de segurança. Por predefinição, o filtro de rastreio de segurança está ativado.
`-time-enabled integer`	Você pode especificar um tempo limite para o filtro, após o qual ele é desativado.

Passos

1. Criar um filtro de rastreamento de segurança:

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

   `filter_parameters` é uma lista de parâmetros de filtro opcionais.

   Para obter mais informações, consulte as páginas man para o comando.

2. Verifique a entrada do filtro de rastreamento de segurança:

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

Exemplos

O comando a seguir cria um filtro de rastreamento de segurança para qualquer usuário que acesse um arquivo com um caminho de compartilhamento do `\\server\share1\dir1\dir2\file.txt` endereço IP 10.10.10.7. O filtro usa um caminho completo para a `-path` opção. O endereço IP do cliente usado para acessar dados é 10.10.10.7. O filtro expira após 30 minutos:

```
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       -
```

O comando a seguir cria um filtro de rastreamento de segurança usando um caminho relativo para a `-path` opção. O filtro rastreia o acesso de um usuário do Windows chamado "joe". Joe está acessando um arquivo com um caminho de compartilhamento `\\server\share1\dir1\dir2\file.txt` . Os rastreamentos de filtro permitem e negam eventos:

```
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
```

Exibir informações sobre filtros de rastreamento de segurança

Você pode exibir informações sobre filtros de rastreamento de segurança configurados na máquina virtual de armazenamento (SVM). Isso permite que você veja quais tipos de eventos de acesso cada filtro rastreia.

Passo

1. Exiba informações sobre entradas de filtro de rastreamento de segurança usando o `vserver security trace filter show` comando.

   Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Exemplos

O comando a seguir exibe informações sobre todos os filtros de rastreamento de segurança no 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
```

Apresentar resultados do rastreio de segurança

Você pode exibir os resultados do rastreamento de segurança gerados para operações de arquivo que correspondam aos filtros de rastreamento de segurança. Use os resultados para validar a configuração de segurança de acesso a arquivos ou para solucionar problemas de acesso a arquivos SMB e NFS.

O que você vai precisar

Um filtro de rastreamento de segurança habilitado deve existir e as operações devem ter sido executadas a partir de um cliente SMB ou NFS que corresponda ao filtro de rastreamento de segurança para gerar resultados de rastreamento de segurança.

Sobre esta tarefa

Você pode exibir um resumo de todos os resultados do rastreamento de segurança ou personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando os resultados do rastreamento de segurança contêm um grande número de Registros.

Se não especificar nenhum dos parâmetros opcionais, é apresentado o seguinte:

- Nome da máquina virtual de storage (SVM)
- Nome do nó
- Número do índice de rastreamento de segurança
- Estilo de segurança
- Caminho
- Motivo
- Nome de utilizador

  O nome de utilizador é apresentado consoante a configuração do filtro de rastreio:

Se o filtro estiver configurado…	Então…
Com um nome de usuário UNIX	O resultado do rastreamento de segurança exibe o nome de usuário UNIX.
Com um nome de usuário do Windows	O resultado do rastreamento de segurança exibe o nome de usuário do Windows.
Sem um nome de usuário	O resultado do rastreamento de segurança exibe o nome de usuário do Windows.

Você pode personalizar a saída usando parâmetros opcionais. Alguns dos parâmetros opcionais que você pode usar para restringir os resultados retornados na saída do comando incluem o seguinte:

Parâmetro opcional	Descrição
`-fields field_name, ...`	Exibe a saída nos campos que você escolher. Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.
`-instance`	Exibe informações detalhadas sobre eventos de rastreamento de segurança. Use este parâmetro com outros parâmetros opcionais para exibir informações detalhadas sobre os resultados específicos do filtro.
`-node node_name`	Exibe informações somente sobre eventos no nó especificado.
`-vserver vserver_name`	Exibe informações somente sobre eventos na SVM especificada.
`-index integer`	Exibe informações sobre os eventos que ocorreram como resultado do filtro correspondente ao número de índice especificado.
`-client-ip IP_address`	Exibe informações sobre os eventos que ocorreram como resultado do acesso ao arquivo a partir do endereço IP do cliente especificado.
`-path path`	Exibe informações sobre os eventos que ocorreram como resultado do acesso de arquivos ao caminho especificado.
`-user-name user_name`	Exibe informações sobre os eventos que ocorreram como resultado do acesso a arquivos pelo usuário especificado do Windows ou UNIX.
`-security-style security_style`	Exibe informações sobre os eventos ocorridos em sistemas de arquivos com o estilo de segurança especificado.

Consulte a página man para obter informações sobre outros parâmetros opcionais que você pode usar com o comando.

Passo

1. Exiba os resultados do filtro de rastreamento de segurança usando o `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/
   ```

Modificar filtros de rastreamento de segurança

Se você quiser alterar os parâmetros de filtro opcionais usados para determinar quais eventos de acesso são rastreados, você pode modificar os filtros de rastreamento de segurança existentes.

Sobre esta tarefa

Você deve identificar qual filtro de rastreamento de segurança deseja modificar especificando o nome da máquina virtual de armazenamento (SVM) no qual o filtro é aplicado e o número de índice do filtro. Você pode modificar todos os parâmetros de filtro opcionais.

Passos

1. Modificar um filtro de rastreamento de segurança:

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

   - `vserver_name` É o nome do SVM no qual você deseja aplicar um filtro de rastreamento de segurança.
   - `index_number` é o número de índice que você deseja aplicar ao filtro. Os valores permitidos para este parâmetro são de 1 a 10.
   - `filter_parameters` é uma lista de parâmetros de filtro opcionais.

2. Verifique a entrada do filtro de rastreamento de segurança:

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

Exemplo

O comando a seguir modifica o filtro de rastreamento de segurança com o índice número 1. O filtro rastreia eventos para qualquer usuário acessando um arquivo com um caminho de compartilhamento

`\\server\share1\dir1\dir2\file.txt` a partir de qualquer endereço IP. O filtro usa um caminho completo para a `-path` opção. Os rastreamentos de filtro permitem e negam eventos:

```
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
```

Excluir filtros de rastreamento de segurança

Quando você não precisa mais de uma entrada de filtro de rastreamento de segurança, você pode excluí-lo. Como você pode ter um máximo de 10 filtros de rastreamento de segurança por máquina virtual de armazenamento (SVM), excluir filtros desnecessários permite criar novos filtros se você atingir o máximo.

Sobre esta tarefa

Para identificar de forma exclusiva o filtro de rastreamento de segurança que você deseja excluir, você deve especificar o seguinte:

- O nome do SVM ao qual o filtro de rastreamento é aplicado
- O número do índice do filtro do traçado

Passos

1. Identifique o número do índice do filtro da entrada do filtro de rastreamento de segurança que você deseja excluir:

   ```
   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. Usando as informações do número do índice do filtro da etapa anterior, exclua a entrada do filtro:

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

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

3. Verifique se a entrada do filtro de rastreamento de segurança foi excluída:

   `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
```

Eliminar registos de rastreio de segurança

Depois de terminar de usar um Registro de rastreamento de filtro para verificar a segurança do acesso ao arquivo ou para solucionar problemas de acesso ao cliente SMB ou NFS, você pode excluir o Registro de rastreamento de segurança do log de rastreamento de segurança.

Sobre esta tarefa

Antes de poder eliminar um registo de rastreio de segurança, tem de saber o número de sequência do registo.

> Cada máquina virtual de storage (SVM) pode armazenar no máximo 128 Registros de rastreamento. Se o máximo for atingido na SVM, os Registros de rastreamento mais antigos serão excluídos automaticamente à medida que novos forem adicionados. Se você não quiser excluir manualmente os Registros de rastreamento neste SVM, você pode permitir que o ONTAP exclua automaticamente os resultados de rastreamento mais antigos depois que o máximo for atingido para abrir espaço para novos resultados.

Passos

1. Identifique o número de sequência do registo que pretende eliminar:

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

2. Eliminar o registo de rastreio de segurança:

   ```
   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` é o nome do nó do cluster no qual ocorreu o evento de rastreamento de permissões que você deseja excluir.

     Este é um parâmetro obrigatório.

   - `-vserver vserver_name` É o nome do SVM no qual ocorreu o evento de rastreamento de permissões que você deseja excluir.

     Este é um parâmetro obrigatório.

   - `-seqnum integer` é o número de sequência do evento de registo que pretende eliminar.

     Este é um parâmetro obrigatório.

Eliminar todos os registos de rastreio de segurança

Se você não quiser manter nenhum dos Registros de rastreamento de segurança existentes, você pode excluir todos os Registros em um nó com um único comando.

Passo

1. Eliminar todos os registos de rastreio de segurança:

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

   - `-node node_name` é o nome do nó do cluster no qual ocorreu o evento de rastreamento de permissões que você deseja excluir.
   - `-vserver vserver_name` É o nome da máquina virtual de armazenamento (SVM) na qual ocorreu o evento de rastreamento de permissões que você deseja excluir.

Informações sobre direitos autorais

Informações sobre marcas comerciais