セキュリティトレースを実行します
ONTAP 9

NetApp
April 24, 2024

目次

セキュリティトレースを実行します

セキュリティトレースの概要を実行します

セキュリティトレースの実行では、セキュリティトレースフィルタの作成、フィルタ条件の確認、フィルタ条件に一致する SMB クライアントまたは NFS クライアントへのアクセス要求の生成、トレース結果の表示などを行います。

セキュリティフィルタを使用してトレース情報をキャプチャしたあと、フィルタを変更して再利用するか、不要になった場合は無効にすることができます。フィルタトレース結果を表示および分析したあと、その結果が不要になった場合は削除できます。

セキュリティトレースフィルタを作成します

Storage Virtual Machine （ SVM ）で SMB および NFS のクライアント処理を検出し、フィルタに一致するすべてのアクセスチェックをトレースするセキュリティトレースフィルタを作成できます。セキュリティトレースの結果を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

vserver security trace filter create コマンドには 2 つの必須パラメータがあります。

必須パラメータ	説明
`-vserver vserver_name`	SVM 名 _ セキュリティトレースフィルタを適用するファイルやフォルダが格納されている SVM の名前。
`-index index_number`	フィルタインデックス番号 _ フィルタに適用するインデックス番号。トレースフィルタは SVM ごとに 10 個まで使用できます。このパラメータに指定できる値は 1~10 です。

さまざまなオプションのフィルタパラメータでセキュリティトレースフィルタをカスタマイズして、セキュリティトレースによって生成された結果を絞り込むことができます。

フィルタパラメータ	説明
`-client-ip IP_Address`	IP アドレスを指定します。この IP アドレスから SVM にアクセスしているユーザが対象となります。

-path path	パーミッショントレースフィルタを適用するパスを指定します。の値 -path 次のいずれかの形式を使用できます。 • 共有またはエクスポートのルートから始まる完全なパス • 共有のルートに対する相対パス パス値では、 NFS 形式のディレクトリ UNIX 形式のディレクトリ区切り文字を使用する必要があります。
-windows-name win_user_name または -unix -name``unix_user_name	アクセス要求をトレースする対象の Windows ユーザ名または UNIX ユーザ名を指定できます。ユーザ名変数では大文字と小文字は区別されません。同じフィルタで Windows ユーザ名と UNIX ユーザ名の両方を指定することはできません。 トレースできるのは SMB と NFS のアクセスイベントだけですが、 mixed セキュリティ形式または UNIX セキュリティ形式のデータに対してアクセスチェックを実行するときに、マッピングされた UNIX ユーザおよび UNIX グループが使用されることがあります。
-trace-allow {yes	no}
セキュリティトレースフィルタでは、拒否イベントのトレースは常に有効です。必要に応じて、許可イベントをトレースすることもできます。許可イベントをトレースするには、このパラメータをに設定します yes。	-enabled {enabled
disabled}	セキュリティトレースフィルタを有効または無効にすることができます。デフォルトでは、セキュリティトレースフィルタは有効になっています。
-time-enabled integer	フィルタのタイムアウトを指定できます。指定した時間が経過すると、フィルタは無効になります。

手順

1. セキュリティトレースフィルタを作成します。

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

   filter_parameters は、オプションのフィルタパラメータのリストです。

   詳細については、コマンドのマニュアルページを参照してください。

2. セキュリティトレースフィルタのエントリを確認します。

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

例

次のコマンドは、共有パスのファイルにアクセスするすべてのユーザを対象とするセキュリティトレースフィルタを作成します `\\server\share1\dir1\dir2\file.txt` IPアドレス10.10.10.7から。フィルタはに完全なパスを使用します `-path` オプションデータへのアクセスに使用されるクライアントの IP アドレスは 10.10.10.7 です。フィルタは 30 分後にタイムアウトします。

```
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       -
```

次のコマンドは、の相対パスを使用してセキュリティトレースフィルタを作成します `-path` オプションこのフィルタは、「 joe 」という名前の Windows ユーザのアクセスをトレースします。Joeは共有パスのファイルにアクセスしています `\\server\share1\dir1\dir2\file.txt`。許可イベントと拒否イベントをトレースします。

```
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
```

セキュリティトレースフィルタに関する情報を表示します

Storage Virtual Machine （ SVM ）で設定されているセキュリティトレースフィルタに関する情報を表示できます。これにより、各フィルタがトレースするアクセスイベントのタイプを確認できます。

ステップ

1. を使用して、セキュリティトレースフィルタエントリに関する情報を表示します `vserver security`

`trace filter show` コマンドを実行します

このコマンドの使用の詳細については、マニュアルページを参照してください。

例

次のコマンドを実行すると、 SVM vs1 のすべてのセキュリティトレースフィルタに関する情報が表示されます。

```
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
```

セキュリティトレースの結果を表示します

セキュリティトレースフィルタに一致するファイル操作に対して生成されたセキュリティトレースの結果を表示できます。この結果を使用して、ファイルアクセスセキュリティ設定の検証や、 SMB および NFS のファイルアクセスに関する問題のトラブルシューティングを行うことができます。

必要なもの

有効なセキュリティトレースフィルタが存在している必要があり、セキュリティトレースの結果が生成されるように、セキュリティトレースフィルタに一致する SMB クライアントまたは NFS クライアントから操作が実行されている必要があります。

このタスクについて

すべてのセキュリティトレースの結果の概要を表示することも、オプションのパラメータを指定して、出力に表示される情報をカスタマイズすることもできます。これは、多数のレコードがセキュリティトレースの結果に含まれている場合に便利です。

オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- Storage Virtual Machine （ SVM ）名
- ノード名
- セキュリティトレースのインデックス番号
- セキュリティ形式
- パス
- 理由
- ユーザ名

トレースフィルタの設定に応じて、ユーザ名が表示されます。

フィルタの設定方法	作業
UNIX ユーザ名を使用する場合	UNIX ユーザ名が表示されます。
Windows ユーザ名を使用	Windows ユーザ名が表示されます。
ユーザ名を使用しない	Windows ユーザ名が表示されます。

オプションのパラメータを使用して、出力をカスタマイズできます。コマンド出力で返される結果を絞り込むために使用できるオプションのパラメータには、次のようなものがあります。

オプションのパラメータ	説明
`-fields` `field_name`はい。	選択したフィールドの出力を表示します。このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。
`-instance`	セキュリティトレースイベントに関する詳細情報を表示します。このパラメータを他のオプションのパラメータとともに使用して、特定のフィルタ結果に関する詳細情報を表示します。
`-node node_name`	指定したノード上のイベントに関する情報のみを表示します。
`-vserver vserver_name`	指定した SVM 上のイベントに関する情報のみを表示します。
`-index integer`	指定したインデックス番号に対応するフィルタの結果として発生したイベントに関する情報を表示します。
`-client-ip IP_address`	指定したクライアント IP アドレスからのファイルアクセスの結果として発生したイベントに関する情報を表示します。
`-path path`	指定したパスへのファイルアクセスの結果として発生したイベントに関する情報を表示します。
`-user-name user_name`	指定した Windows ユーザまたは UNIX ユーザによるファイルアクセスの結果として発生したイベントに関する情報を表示します。
`-security-style security_style`	指定したセキュリティ形式のファイルシステムで発生したイベントに関する情報を表示します。

コマンドで使用できる他のオプションのパラメータについては、マニュアルページを参照してください。

ステップ

1. を使用して、セキュリティトレースフィルタの結果を表示します `vserver security trace trace-`

`result show` コマンドを実行します

```
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/
```

セキュリティトレースフィルタを変更する

トレースされたアクセスイベントを特定する際に使用するオプションのフィルタパラメータを変更するには、既存のセキュリティトレースフィルタを変更します。

このタスクについて

変更するセキュリティトレースフィルタを特定するには、フィルタを適用した Storage Virtual Machine （ SVM ）の名前とフィルタのインデックス番号を指定します。オプションのフィルタパラメータはすべて変更できます。

手順

1. セキュリティトレースフィルタを変更します。

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

   - `vserver_name` は、セキュリティトレースフィルタを適用するSVMの名前です。
   - `index_number` は、フィルタに適用するインデックス番号です。このパラメータに指定できる値は 1~10 です。
   - `filter_parameters` は、オプションのフィルタパラメータのリストです。

2. セキュリティトレースフィルタのエントリを確認します。

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

例

次の例は、インデックス番号 1 のセキュリティトレースフィルタを変更します。このフィルタは、共有パスのファイルにアクセスしているすべてのユーザのイベントをトレースします `\\server\share1\dir1\dir2\file.txt` 任意のIPアドレスから。フィルタはに完全なパスを使用します `-path` オプション許可イベントと拒否イベントをトレースします。

```
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
```

セキュリティトレースフィルタを削除します

セキュリティトレースフィルタエントリが不要になった場合は削除できます。セキュリティトレースフィルタは Storage Virtual Machine （ SVM ）ごとに 10 個までしか使用できないので、上限に達した場合は、不要なフィルタを削除すると、新しいフィルタを作成できます。

このタスクについて

削除するセキュリティトレースフィルタを一意に識別するには、次の項目を指定する必要があります。

- トレースフィルタが適用されている SVM の名前
- トレースフィルタのフィルタインデックス番号

手順

1. 削除するセキュリティトレースフィルタエントリのフィルタインデックス番号を確認します。

   ```
   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. 前の手順で確認したフィルタインデックス番号を使用して、フィルタエントリを削除します。

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

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

3. セキュリティトレースフィルタエントリが削除されたことを確認します。

```
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
```

セキュリティトレースレコードを削除します

セキュリティトレースレコードを使用したファイルアクセスセキュリティの検証や、SMB または NFS のクライアントアクセスに関する問題のトラブルシューティングが完了したら、セキュリティトレースのログからセキュリティトレースレコードを削除できます。

このタスクについて

セキュリティトレースレコードを削除する前に、レコードのシーケンス番号を確認しておく必要があります。

> 各 Storage Virtual Machine （ SVM ）には、最大 128 件のトレースレコードを保存できます。SVM でこの上限に達した場合、最も古いトレースレコードが自動的に削除されて、新しいレコードが追加されます。したがって、 SVM のトレースレコードを手動で削除しなくても、上限に達したときに、 ONTAP によって自動的に最も古いトレース結果を削除して新しい結果用のスペースを確保することができます。

手順

1. 削除するレコードのシーケンス番号を指定します。

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

2. セキュリティトレースレコードを削除します。

```
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` は、削除するパーミッショントレーシングイベントが発生したクラスタノードの

名前です。

これは必須パラメータです。

- `-vserver vserver_name` は、削除対象のパーミッショントレーシングイベントが発生したSVMの名前です。

  これは必須パラメータです。

- `-seqnum integer` は、削除するログイベントのシーケンス番号です。

  これは必須パラメータです。

すべてのセキュリティトレースレコードを削除します

既存のセキュリティトレースレコードが不要である場合は、 1 つのコマンドで特定のノード上のレコードをすべて削除できます。

ステップ

1. すべてのセキュリティトレースレコードを削除します。

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

   - `-node node_name` は、削除するパーミッショントレーシングイベントが発生したクラスタノードの名前です。
   - `-vserver vserver_name` は、削除するパーミッショントレーシングイベントが発生したStorage Virtual Machine（SVM）の名前です。