セキュリティトレースの実行
ONTAP 9

NetApp
December 20, 2024

目次

セキュリティトレースの実行

セキュリティトレースの概要の実行

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する

Storage Virtual Machine（SVM）でSMBと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、設定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。

タスクの内容

vserver security trace filter createコマンドには、次の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。

オプションのフィルタパラメータをいくつか使用すると、セキュリティトレースのフィルタをカスタマイズして、セキュリティトレースの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です。

`-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`には、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パス • 共有のルートに対する相対パス パス値には、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。同じフィルタに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およびNFSのアクセスイベントですが、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が常に有効になります。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`yes`ます。	`-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、IPアドレス10.10.10.7から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したセキュリティトレースフィルタを作成し `\\server\share1\dir1\dir2\file.txt`ます。フィルタでは、オプションに完全なパスが使用され `-path`ます。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、オプション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 `-path`ます。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する

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. コマンドを使用して、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`。

このコマンドの使用方法の詳細については、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クライアントから処理が実行されている必要があります。

タスクの内容

すべてのセキュリティトレース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、出力に表示する情報をカスタマイズすることもできます。これは、セキュリティトレースの結果に多数のレコードが含まれている場合に役立ちます。

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	そしたら…。
UNIXユーザ名を使用	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その他のオプション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. コマンドを使用して、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。

```
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します。

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。

タスクの内容

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、任意のIPアドレスから共有パスを持つ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`\\server\share1\dir1\dir2\file.txt`ます。フィルタでは、オプションに完全なパスが使用され `-path`ます。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ため、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。

タスクの内容

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する

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。

タスクの内容

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格納できます。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する

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。

著作権に関する情報

商標に関する情報