Perform security traces

ONTAP 9

NetApp
February 20, 2023

Table of Contents

Perform security traces

Perform security traces overview

Performing a security trace involves creating a security trace filter, verifying the filter criteria, generating access requests on an SMB or NFS client that match filter criteria, and viewing the results.

After you are finished using a security filter to capture trace information, you can modify the filter and reuse it, or disable it if you no longer need it. After viewing and analyzing the filter trace results, you can then delete them if they are no longer needed.

Create security trace filters

You can create security trace filters that detect SMB and NFS client operations on storage virtual machines (SVMs)and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

About this task

There are two required parameters for the vserver security trace filter create command:

Required parameters	Description
`-vserver vserver_name`	*SVM name* The name of the SVM that contains the files or folders on which you want to apply the security trace filter.
`-index index_number`	*Filter index number* The index number you want to apply to the filter. You are limited to a maximum of 10 trace filters per SVM. The allowed values for this parameter are 1 through 10.

A number of optional filter parameters enable you to customize the security trace filter so that you can narrow down the results produced by the security trace:

Filter parameter	Description
`-client-ip IP_Address`	This filter specifies the IP address from which the user is accessing the SVM.

`-path path`	This filter specifies the path on which to apply the permission trace filter. The value for `-path` can use either of the following formats: • The complete path, starting from the root of the share or export • A partial path, relative to the root of the share You must use NFS style directory UNIX-style directory separators in the path value.
`-windows-name win_user_name` or `-unix -name``unix_user_name`	You can specify either the Windows user name or UNIX user name whose access requests you want to trace. The user name variable is case insensitive. You cannot specify both a Windows user name and a UNIX user name in the same filter. (i) Even though you can trace SMB and NFS access events, the mapped UNIX user and the mapped UNIX users' groups might be used when performing access checks on mixed or UNIX security-style data.
`-trace-allow {yes|no}`	Tracing for deny events is always enabled for a security trace filter. You can optionally trace allow events. To trace allow events, you set this parameter to `yes`.
`-enabled {enabled|disabled}`	You can enable or disable the security trace filter. By default, the security trace filter is enabled.
`-time-enabled integer`	You can specify a timeout for the filter, after which it is disabled.

Steps

1. Create a security trace filter:

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

   `filter_parameters` is a list of optional filter parameters.

   For more information, see the man pages for the command.

2. Verify the security trace filter entry:

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

Examples

The following command creates a security trace filter for any user accessing a file with a share path `\\server\share1\dir1\dir2\file.txt` from the IP address 10.10.10.7. The filter uses a complete path for the `-path` option. The client's IP address used to access data is 10.10.10.7. The filter times out after 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       -
```

The following command creates a security trace filter using a relative path for the -path option. The filter traces access for a Windows user named "joe". Joe is accessing a file with a share path \\server\share1\dir1\dir2\file.txt. The filter traces allow and deny events:

```
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
```

Display information about security trace filters

You can display information about security trace filters configured on your storage virtual machine (SVM). This enables you to see which types of access events each filter traces.

Step

1. Display information about security trace filter entries by using the `vserver security trace filter show` command.

   For more information about using this command, see the man pages.

Examples

The following command displays information about all security trace filters on 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
```

Display security trace results

You can display the security trace results generated for file operations that match security trace filters. You can use the results to validate your file access security configuration or to troubleshoot SMB and NFS file access issues.

What you'll need

An enabled security trace filter must exist and operations must have been performed from an SMB or NFS client that matches the security trace filter to generate security trace results.

About this task

You can display a summary of all security trace results, or you can customize what information is displayed in the output by specifying optional parameters. This can be helpful when the security trace results contain a large number of records.

If you do not specify any of the optional parameters, the following is displayed:

- storage virtual machine (SVM) name

- Node name

- Security trace index number

- Security style

- Path

- Reason

- User name

  The user name is displayed depending on how the trace filter is configured:

If the filter is configured…	Then…
With a UNIX user name	The security trace result displays the UNIX user name.
With a Windows user name	The security trace result displays the Windows user name.
Without a user name	The security trace result displays the Windows user name.

You can customize the output by using optional parameters. Some of the optional parameters that you can use

to narrow the results returned in the command output include the following:

Optional parameter	Description
`-fields field_name, …`	Displays output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters.
`-instance`	Displays detailed information about security trace events. Use this parameter with other optional parameters to display detailed information about specific filter results.
`-node node_name`	Displays information only about events on the specified node.
`-vserver vserver_name`	Displays information only about events on the specified SVM.
`-index integer`	Displays information about the events that occurred as a result of the filter corresponding to the specified index number.
`-client-ip IP_address`	Displays information about the events that occurred as a result of file access from the specified client IP address.
`-path path`	Displays information about the events that occurred as a result of file access to the specified path.
`-user-name user_name`	Displays information about the events that occurred as a result of file access by the specified Windows or UNIX user.
`-security-style security_style`	Displays information about the events that occurred on file systems with the specified security style.

See the man page for information about other optional parameters that you can use with the command.

Step

1. Display security trace filter results by using the `vserver security trace trace-result show` command.

   ```
   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/
```

Modify security trace filters

If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

About this task

You must identify which security trace filter you want to modify by specifying the storage virtual machine (SVM) name on which the filter is applied and the index number of the filter. You can modify all the optional filter parameters.

Steps

1. Modify a security trace filter:

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

   ° `vserver_name` is the name of the SVM on which you want to apply a security trace filter.

   ° `index_number` is the index number that you want to apply to the filter. The allowed values for this parameter are 1 through 10.

   ° `filter_parameters` is a list of optional filter parameters.

2. Verify the security trace filter entry:

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

Example

The following command modifies the security trace filter with the index number 1. The filter traces events for any user accessing a file with a share path `\\server\share1\dir1\dir2\file.txt` from any IP address. The filter uses a complete path for the `-path` option. The filter traces allow and deny events:

```
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
```

Delete security trace filters

When you no longer need a security trace filter entry, you can delete it. Because you can
have a maximum of 10 security trace filters per storage virtual machine (SVM), deleting
unneeded filters enables you to create new filters if you have reached the maximum.

About this task

To uniquely identify the security trace filter that you want to delete, you must specify the following:

- The name of the SVM to which the trace filter is applied
- The filter index number of the trace filter

Steps

1. Identify the filter index number of the security trace filter entry you want to delete:

   `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. Using the filter index number information from the previous step, delete the filter entry:

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

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

3. Verify that the security trace filter entry is deleted:

```
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
```

Delete security trace records

After you finish using a filter trace record to verify file access security or to troubleshoot SMB or NFS client access issues, you can delete the security trace record from the security trace log.

About this task

Before you can delete a security trace record, you must know the record's sequence number.

ⓘ Each storage virtual machine (SVM) can store a maximum of 128 trace records. If the maximum is reached on the SVM, the oldest trace records are automatically deleted as new ones are added. If you do not want to manually delete trace records on this SVM, you can let ONTAP automatically delete the oldest trace results after the maximum is reached to make room for new results.

Steps

1. Identify the sequence number of the record you want to delete:

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

2. Delete the security trace record:

```
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` is the name of the cluster node on which the permission tracing event that you want to delete occurred.

  This is a required parameter.

- ◦ `-vserver vserver_name` is the name of the SVM on which the permission tracing event that you want to delete occurred.

  This is a required parameter.

- ◦ `-seqnum integer` is the sequence number of the log event that you want to delete.

  This is a required parameter.

Delete all security trace records

If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

Step

1. Delete all security trace records:

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

   - ◦ `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.
   - ◦ `-vserver vserver_name` is the name of the storage virtual machine (SVM) on which the permission tracing event that you want to delete occurred.