



# **Führen Sie Sicherheitspuren durch ONTAP 9**

NetApp  
April 24, 2024

# Inhalt

- Führen Sie Sicherheitspuren durch ..... 1
  - Übersicht über Sicherheitspuren durchführen ..... 1
  - Erstellen von Sicherheitsverfolgungsfiltern ..... 1
  - Informationen zu Sicherheitsverfolgungsfiltern anzeigen ..... 3
  - Zeigen Sie die Ergebnisse der Sicherheitspurenverfolgung an ..... 4
  - Ändern Sie die Filter für die Sicherheitsverfolgung ..... 6
  - Löschen Sie die Sicherheitsverfolgungsfilter ..... 7
  - Löschen von Sicherheits-Trace-Datensätzen ..... 8
  - Löschen Sie alle Sicherheits-Trace-Datensätze ..... 9

# Führen Sie Sicherheitspuren durch

## Übersicht über Sicherheitspuren durchführen

Beim Durchführen eines Sicherheitspurenfilters werden ein Sicherheitsverfolgungsfilter erstellt, die Filterkriterien überprüft, Zugriffsanfragen auf einem SMB- oder NFS-Client generiert, die den Filterkriterien entsprechen, und die Ergebnisse angezeigt.

Nachdem Sie mit einem Sicherheitsfilter die Trace-Informationen erfasst haben, können Sie den Filter ändern und erneut verwenden oder deaktivieren, wenn Sie ihn nicht mehr benötigen. Nach dem Anzeigen und Analysieren der Filter-Trace-Ergebnisse können Sie sie löschen, wenn sie nicht mehr benötigt werden.

## Erstellen von Sicherheitsverfolgungsfiltern

Sie können Filter für Sicherheitsspuren erstellen, die SMB- und NFS-Client-Vorgänge auf Storage Virtual Machines (SVMs) erkennen und alle Zugriffsprüfungen verfolgen, die dem Filter entsprechen. Sie können die Ergebnisse aus Sicherheitspuren verwenden, um Ihre Konfiguration zu validieren oder um Zugriffsprobleme zu beheben.


### Über diese Aufgabe

Für den Befehl `vserver Security trace Filter create` gibt es zwei erforderliche Parameter:

Erforderliche Parameter	Beschreibung
<code>-vserver vserver_name</code>	<i>SVM Name</i>  Der Name der SVM, die die Dateien oder Ordner enthält, auf denen Sie den Filter für die Sicherheitsverfolgung anwenden möchten.
<code>-index index_number</code>	<i>Indexnummer Filter</i>  Die Indexnummer, die auf den Filter angewendet werden soll. Sie dürfen pro SVM maximal 10 Trace-Filter verwenden. Die zulässigen Werte für diesen Parameter sind 1 bis 10.

Mit einer Reihe optionaler Filterparameter können Sie den Sicherheitsspurfilter so anpassen, dass Sie die Ergebnisse des Sicherheitspurenfilters eingrenzen können:

Filterparameter	Beschreibung
<code>-client-ip IP_Address</code>	Dieser Filter gibt die IP-Adresse an, von der der Benutzer auf die SVM zugreift.

<code>-path path</code>	<p>Dieser Filter gibt den Pfad an, auf den der Berechtigungs-Trace-Filter angewendet werden soll. Der Wert für <code>-path</code> Es stehen folgende Formate zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Der vollständige Pfad, beginnend mit dem Stammverzeichnis der Freigabe oder des Exports</li> <li>• Ein partieller Pfad, relativ zur Wurzel des Shares</li> </ul> <p>Im Pfadwert müssen Sie die Verzeichnistrennzeichen für das NFS-Style-Verzeichnis UNIX-Stil verwenden.</p>
<code>-windows-name win_user_name</code> Oder <code>-unix</code> <code>-name`unix_user_name</code>	<p>Sie können entweder den Windows-Benutzernamen oder den UNIX-Benutzernamen angeben, dessen Zugriffsanfragen Sie nachverfolgen möchten. Die Groß-/Kleinschreibung der Variable für den Benutzernamen wird nicht berücksichtigt. Sie können keinen Windows-Benutzernamen und keinen UNIX-Benutzernamen im selben Filter angeben.</p> <div>  <p>Auch wenn Sie SMB- und NFS-Zugriffseignisse verfolgen können, können der zugewiesene UNIX Benutzer und die zugeordneten UNIX Benutzergruppen verwendet werden, wenn Zugriffsprüfungen für gemischte oder UNIX-Sicherheitsdaten durchgeführt werden.</p> </div>
<code>-trace-allow {yes</code>	<code>no}</code>
<p>Für einen Sicherheits-Trace-Filter ist immer die Verfolgung von Deny-Ereignissen aktiviert. Sie können optional Ereignisse zulassen nachverfolgen. Um Ereignisse zuzulassen, legen Sie diesen Parameter auf fest <code>yes</code>.</p>	<code>-enabled {enabled</code>
<code>disabled}</code>	<p>Sie können den Filter für die Sicherheitsverfolgung aktivieren oder deaktivieren. Standardmäßig ist der Filter Security Trace aktiviert.</p>
<code>-time-enabled integer</code>	<p>Sie können eine Zeitüberschreitung für den Filter angeben, nach der er deaktiviert ist.</p>

## Schritte

### 1. Erstellen eines Sicherheits-Trace-Filters:

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

`filter_parameters` Ist eine Liste der optionalen Filterparameter.

Weitere Informationen finden Sie auf den man-Pages für den Befehl.

## 2. Überprüfen Sie den Eintrag des Sicherheits-Trace-Filters:

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

### Beispiele

Mit dem folgenden Befehl wird ein Security Trace Filter für jeden Benutzer erstellt, der auf eine Datei mit einem Freigabepfad zugreift `\\server\share1\dir1\dir2\file.txt` Aus der IP-Adresse 10.10.10.7. Der Filter verwendet einen vollständigen Pfad für den `-path` Option. Die IP-Adresse des Clients, die für den Zugriff auf Daten verwendet wird, lautet 10.10.10.7. Der Filter wird nach 30 Minuten ausgezeit:

```
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	-

Mit dem folgenden Befehl wird ein Security Trace Filter unter Verwendung eines relativen Pfads für das erstellt `-path` Option. Der Filter verfolgt den Zugriff für einen Windows-Benutzer namens „joe“. Joe greift auf eine Datei mit einem Freigabepfad zu `\\server\share1\dir1\dir2\file.txt`. Die Filterspuren erlauben und verweigern Ereignisse:

```
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
```

## Informationen zu Sicherheitsverfolgungsfiltern anzeigen

Sie können Informationen zu den auf Ihrer Storage Virtual Machine (SVM) konfigurierten Sicherheitstrace-Filtern anzeigen. So können Sie sehen, welche Arten von Zugriffsereignissen die einzelnen Filterspuren anzeigen.

## Schritt

1. Zeigen Sie mithilfe der Informationen zu den Einträgen von Sicherheitsverfolgungsfiltern an `vserver security trace filter show` Befehl.

Weitere Informationen über diese Verwendung dieses Befehls finden Sie in den man-Pages.

## Beispiele

Mit dem folgenden Befehl werden Informationen zu allen SicherheitsTrace-Filtern in SVM vs1 angezeigt:

```
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					

## Zeigen Sie die Ergebnisse der Sicherheitspurenverfolgung an

Sie können die für Dateivorgänge generierten Ergebnisse von Sicherheitspuren anzeigen, die mit den Filtern von Sicherheitsnachverfolgung übereinstimmen. Anhand der Ergebnisse können Sie die Sicherheitskonfiguration für den Dateizugriff validieren oder Probleme mit dem SMB- und NFS-Dateizugriff beheben.

### Was Sie benötigen

Es muss ein aktivierter Filter für Sicherheitsnachverfolgung vorhanden sein, und Vorgänge müssen von einem SMB- oder NFS-Client ausgeführt werden, der mit dem Security Trace-Filter übereinstimmt, um Ergebnisse von Sicherheitspuren zu generieren.

### Über diese Aufgabe

Sie können eine Zusammenfassung aller Ergebnisse von Sicherheitspuren anzeigen oder durch Angabe optionaler Parameter anpassen, welche Informationen in der Ausgabe angezeigt werden. Dies kann hilfreich sein, wenn die Ergebnisse der Sicherheitspurenverfolgung eine große Anzahl von Datensätzen enthalten.

Wenn Sie keinen der optionalen Parameter angeben, wird Folgendes angezeigt:

- Name der Storage Virtual Machine (SVM)
- Node-Name
- Indexnummer der Sicherheitsspur
- Sicherheitsstil
- Pfad
- Grund
- Benutzername

Der Benutzername wird je nach Konfiguration des Trace-Filters angezeigt:

Wenn der Filter konfiguriert ist...	Dann...
Mit einem UNIX-Benutzernamen	Das Ergebnis der Sicherheitsverfolgung zeigt den UNIX-Benutzernamen an.
Mit einem Windows-Benutzernamen	Das Ergebnis der Sicherheitsverfolgung zeigt den Windows-Benutzernamen an.
Ohne Benutzernamen	Das Ergebnis der Sicherheitsverfolgung zeigt den Windows-Benutzernamen an.

Sie können die Ausgabe mit optionalen Parametern anpassen. Einige der optionalen Parameter, mit denen Sie die in der Befehlsausgabe zurückgegebenen Ergebnisse eingrenzen können, umfassen die folgenden:

Optionaler Parameter	Beschreibung
<code>-fields field_name, ...</code>	Zeigt die Ausgabe der ausgewählten Felder an. Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.
<code>-instance</code>	Zeigt detaillierte Informationen zu Sicherheits-Trace-Ereignissen an. Verwenden Sie diesen Parameter mit anderen optionalen Parametern, um detaillierte Informationen zu bestimmten Filterergebnissen anzuzeigen.
<code>-node node_name</code>	Zeigt nur Informationen zu Ereignissen auf dem angegebenen Node an.
<code>-vserver vserver_name</code>	Zeigt nur Informationen zu Ereignissen auf der angegebenen SVM an.
<code>-index integer</code>	Zeigt Informationen zu den Ereignissen an, die als Ergebnis des Filters der angegebenen Indexnummer aufgetreten sind.
<code>-client-ip IP_address</code>	Zeigt Informationen zu den Ereignissen an, die infolge des Dateizugriffs von der angegebenen Client-IP-Adresse aufgetreten sind.
<code>-path path</code>	Zeigt Informationen zu den Ereignissen an, die infolge des Dateizugriffs auf den angegebenen Pfad aufgetreten sind.
<code>-user-name user_name</code>	Zeigt Informationen zu Ereignissen an, die durch den Dateizugriff durch den angegebenen Windows- oder UNIX-Benutzer aufgetreten sind.
<code>-security-style security_style</code>	Zeigt Informationen zu Ereignissen an, die auf Dateisystemen mit dem angegebenen Sicherheitsstil aufgetreten sind.

Informationen zu anderen optionalen Parametern, die Sie mit dem Befehl verwenden können, finden Sie auf der man-Seite.

### Schritt

1. Zeigen Sie die Ergebnisse des Filter für Sicherheitsnachverfolgung mithilfe des `vserver security trace trace-result show` Befehl.

```
vserver security trace trace-result show -user-name domain\user
```

Vserver: vs1

Node	Index	Filter Details	Reason
-----	-----	-----	-----
node1	3	User:domain\user Security Style:mixed Path:/dir1/dir2/	Access denied by explicit ACE
node1	5	User:domain\user Security Style:unix Path:/dir1/	Access denied by explicit ACE

## Ändern Sie die Filter für die Sicherheitsverfolgung

Wenn Sie die optionalen Filterparameter ändern möchten, mit denen ermittelt wird, welche Zugriffsereignisse verfolgt werden, können Sie vorhandene Sicherheits-Trace-Filter ändern.

### Über diese Aufgabe

Sie müssen ermitteln, welchen Sicherheits-Trace-Filter Sie ändern möchten, indem Sie den SVM-Namen (Storage Virtual Machine) angeben, auf den der Filter angewendet wird, und die Indexnummer des Filters. Sie können alle optionalen Filterparameter ändern.

### Schritte

1. Bearbeiten eines Sicherheitsverfolgungsfilters:

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

- `vserver_name` Ist der Name der SVM, auf der Sie einen Sicherheits-Trace-Filter anwenden möchten.
- `index_number` Ist die Indexnummer, die Sie auf den Filter anwenden möchten. Die zulässigen Werte für diesen Parameter sind 1 bis 10.
- `filter_parameters` Ist eine Liste der optionalen Filterparameter.

2. Überprüfen Sie den Eintrag des Sicherheits-Trace-Filters:

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



## Beispiel

Mit dem folgenden Befehl wird der Security Trace Filter mit der Indexnummer 1 geändert. Der Filter verfolgt Ereignisse für jeden Benutzer, der auf eine Datei mit einem Freigabepfad zugreift

\\server\share1\dir1\dir2\file.txt Von einer beliebigen IP-Adresse aus. Der Filter verwendet einen vollständigen Pfad für den -path Option. Die Filterspuren erlauben und verweigern Ereignisse:

```
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
```

## Löschen Sie die Sicherheitsverfolgungsfiler

Wenn Sie keinen Eintrag für den Sicherheits-Trace-Filter mehr benötigen, können Sie ihn löschen. Da Sie maximal 10 Sicherheitsverfolgungsfiler pro Storage Virtual Machine (SVM) verwenden können, können Sie durch das Löschen nicht benötigter Filter neue Filter erstellen, wenn Sie das Maximum erreicht haben.

### Über diese Aufgabe

Um den zu löschenden Sicherheits-Trace-Filter eindeutig zu identifizieren, müssen Sie Folgendes angeben:

- Der Name der SVM, auf die der Trace-Filter angewendet wird
- Die Filterindex-Nummer des Trace-Filters

### Schritte

1. Geben Sie die Filterindex-Nummer des zu löschenden Sicherheits-Trace-Filters an:

```
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. Löschen Sie den Filtereintrag mithilfe der Filterindex-Nummern aus dem vorherigen Schritt:

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

3. Vergewissern Sie sich, dass der Eintrag für den Sicherheits-Trace-Filter gelöscht wurde:

```
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					

## Löschen von Sicherheits-Trace-Datensätzen

Nachdem Sie den Filter-Trace-Datensatz zur Überprüfung der Dateizugriffssicherheit verwendet oder Probleme mit dem Zugriff auf SMB- oder NFS-Clients behoben haben, können Sie den Security Trace-Datensatz aus dem Security Trace-Protokoll löschen.

### Über diese Aufgabe

Bevor Sie einen Sicherheits-Trace-Datensatz löschen können, müssen Sie die Sequenznummer des Datensatzes kennen.



Jede Storage Virtual Machine (SVM) kann maximal 128 Trace-Datensätze speichern. Wird das Maximum auf der SVM erreicht, werden die ältesten Trace-Datensätze automatisch gelöscht, sobald neue hinzugefügt werden. Wenn Sie Trace-Datensätze auf dieser SVM nicht manuell löschen möchten, können Sie ONTAP die ältesten Trace-Ergebnisse automatisch löschen lassen, nachdem das Maximum erreicht wurde, um Platz für neue Ergebnisse zu schaffen.

### Schritte

1. Geben Sie die Sequenznummer des zu löschenden Datensatzes an:

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

## 2. Löschen Sie den Sicherheits-Trace-Datensatz:

```
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` Ist der Name des Cluster-Node, auf dem das Ereignis Berechtigungstrennung, das Sie löschen möchten, stattgefunden hat.

Dies ist ein erforderlicher Parameter.

- `-vserver vserver_name` Ist der Name der SVM, auf der das Ereignis für die Berechtigungsverfolgung, das Sie löschen möchten, stattgefunden hat.

Dies ist ein erforderlicher Parameter.

- `-seqnum integer` Ist die Sequenznummer des Protokollereignisses, das Sie löschen möchten.

Dies ist ein erforderlicher Parameter.

## Löschen Sie alle Sicherheits-Trace-Datensätze

Wenn Sie keine der vorhandenen Sicherheits-Trace-Datensätze speichern möchten, können Sie alle Datensätze auf einem Knoten mit einem einzigen Befehl löschen.

### Schritt

#### 1. Alle Sicherheitsaufzeichnungen löschen:

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

- `-node node_name` Ist der Name des Cluster-Node, auf dem das Ereignis Berechtigungstrennung, das Sie löschen möchten, stattgefunden hat.
- `-vserver vserver_name` Ist der Name der Storage Virtual Machine (SVM), auf der das Ereignis für die Berechtigungsverfolgung, das Sie löschen möchten, stattgefunden hat.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.