



执行安全跟踪 ONTAP 9

NetApp
April 24, 2024

目录

- 执行安全跟踪 1
 - 执行安全跟踪概述 1
 - 创建安全跟踪筛选器 1
 - 显示有关安全跟踪筛选器的信息 3
 - 显示安全跟踪结果 4
 - 修改安全跟踪筛选器 6
 - 删除安全跟踪筛选器 6
 - 删除安全跟踪记录 8
 - 删除所有安全跟踪记录 8

执行安全跟踪

执行安全跟踪概述

执行安全跟踪涉及创建安全跟踪筛选器，验证筛选条件，在符合筛选条件的 SMB 或 NFS 客户端上生成访问请求以及查看结果。

在使用安全筛选器捕获跟踪信息后，您可以修改此筛选器并重复使用它，或者在不再需要时将其禁用。查看并分析筛选器跟踪结果后，如果不再需要，您可以将其删除。

创建安全跟踪筛选器

您可以创建安全跟踪筛选器来检测 Storage Virtual Machine （SVM）上的 SMB 和 NFS 客户端操作，并跟踪与此筛选器匹配的所有访问检查。您可以使用安全跟踪的结果来验证配置或对访问问题进行故障排除。

关于此任务

vserver security trace filter create 命令需要两个参数：

所需参数	Description
-vserver vserver_name	<p>_SVM 名称 _</p> <p>包含要应用安全跟踪筛选器的文件或文件夹的 SVM 的名称。</p>
-index index_number	<p>筛选索引号 _</p> <p>要应用于筛选器的索引编号。每个 SVM 最多只能有 10 个跟踪筛选器。此参数允许的值为 1 到 10 。</p>

您可以使用多个可选筛选器参数自定义安全跟踪筛选器，以便缩小安全跟踪生成的结果范围：

filter 参数	Description
-client-ip IP_Address	此筛选器指定用户从中访问 SVM 的 IP 地址。
-path path	<p>此筛选器指定要应用权限跟踪筛选器的路径。的值 -path 可以使用以下格式之一：</p> <ul style="list-style-type: none">• 从共享或导出的根目录开始的完整路径• 相对于共享根的部分路径 <p>必须在路径值中使用 NFS 模式目录 UNIX 模式目录分隔符。</p>

<code>-windows-name win_user_name</code> 或 <code>-unix</code> <code>-name ``unix_user_name</code>	<p>您可以指定要跟踪其访问请求的 Windows 用户名或 UNIX 用户名。用户名变量不区分大小写。您不能在同一筛选器中同时指定 Windows 用户名和 UNIX 用户名。</p> <div><p>即使您可以跟踪 SMB 和 NFS 访问事件，在对混合或 UNIX 安全模式数据执行访问检查时，也可能会使用映射的 UNIX 用户和映射的 UNIX 用户组。</p></div>
<code>-trace-allow {yes</code>	<code>no}</code>
对于安全跟踪筛选器，始终会启用对拒绝事件的跟踪。您可以选择跟踪允许事件。要跟踪允许事件、请将此参数设置为 yes。	<code>-enabled {enabled</code>
<code>disabled}</code>	您可以启用或禁用安全跟踪筛选器。默认情况下，安全跟踪筛选器处于启用状态。
<code>-time-enabled integer</code>	您可以为筛选器指定超时时间，超过此超时时间后将其禁用。

步骤

1. 创建安全跟踪筛选器：

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

filter_parameters 是可选筛选器参数的列表。

有关详细信息，请参见命令的手册页。

2. 验证安全跟踪筛选器条目：

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

示例

以下命令将为使用共享路径访问文件的任何用户创建安全跟踪筛选器
\\server\share1\dir1\dir2\file.txt 从IP地址10.10.10.7。筛选器将使用的完整路径 -path 选项用于
访问数据的客户端 IP 地址为 10.10.10.7。筛选器在 30 分钟后超时：

```
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	-

以下命令使用的相对路径创建安全跟踪筛选器 -path 选项此筛选器会跟踪名为 "Joe` " 的 Windows 用户的访问权限。Joe正在访问具有共享路径的文件 \\server\share1\dir1\dir2\file.txt。筛选器跟踪允许和拒绝事件：

```
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

```

显示有关安全跟踪筛选器的信息

您可以显示有关在 Storage Virtual Machine （ SVM ） 上配置的安全跟踪筛选器的信息。这样，您可以查看每个筛选器跟踪的访问事件类型。

步骤

1. 使用显示有关安全跟踪筛选器条目的信息 `vserver security trace filter show` 命令：

有关使用此命令的详细信息，请参见手册页。

示例

以下命令显示有关 SVM vs1 上所有安全跟踪筛选器的信息：

```
cluster1::> vsserver security trace filter show -vsserver vs1
Vserver      Index      Client-IP      Path      Trace-Allow
Windows-Name
-----
vs1           1      -      /dir1/dir2/file.txt      yes      -
vs1           2      -      /dir3/dir4/      no
mydomain\joe
```

显示安全跟踪结果

您可以显示为与安全跟踪筛选器匹配的文件操作生成的安全跟踪结果。您可以使用结果验证文件访问安全配置，或者对 SMB 和 NFS 文件访问问题进行故障排除。

您需要的内容

必须存在已启用的安全跟踪筛选器，并且必须已从与安全跟踪筛选器匹配的 SMB 或 NFS 客户端执行操作，才能生成安全跟踪结果。

关于此任务

您可以显示所有安全跟踪结果的摘要，也可以通过指定可选参数来自定义输出中显示的信息。如果安全跟踪结果包含大量记录，则此操作可能会很有用。

如果未指定任何可选参数，则会显示以下内容：

- Storage Virtual Machine （ SVM ） 名称
- Node name
- 安全跟踪索引编号
- 安全风格
- 路径
- reason
- 用户名

根据跟踪筛选器的配置方式显示用户名：

如果筛选器已配置 ...	那么 ...
使用 UNIX 用户名	安全跟踪结果将显示 UNIX 用户名。
使用 Windows 用户名	安全跟踪结果将显示 Windows 用户名。
没有用户名	安全跟踪结果将显示 Windows 用户名。

您可以使用可选参数自定义输出。可用于缩小命令输出中返回的结果范围的一些可选参数包括：

可选参数	Description
-fields field_name, ...	显示所选字段的输出。您可以单独使用此参数，也可以与其他可选参数结合使用。
-instance	显示有关安全跟踪事件的详细信息。将此参数与其他可选参数结合使用可显示有关特定筛选器结果的详细信息。
-node node_name	仅显示有关指定节点上的事件的信息。
-vserver vservice_name	仅显示有关指定 SVM 上的事件的信息。
-index integer	显示有关因与指定索引编号对应的筛选器而发生的事件的信息。
-client-ip IP_address	显示有关从指定客户端 IP 地址访问文件而发生的事件的信息。
-path path	显示有关通过文件访问指定路径而发生的事件的信息。
-user-name user_name	显示有关指定 Windows 或 UNIX 用户访问文件时发生的事件的信息。
-security-style security_style	显示有关使用指定安全模式的文件系统上发生的事件的信息。

有关可与命令结合使用的其他可选参数的信息，请参见手册页。

步骤

1. 使用显示安全跟踪筛选器结果 vservice security trace trace-result show 命令：

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

```
Vservice: 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/
```

修改安全跟踪筛选器

如果要更改用于确定跟踪哪些访问事件的可选筛选器参数，可以修改现有的安全跟踪筛选器。

关于此任务

您必须指定要修改的安全跟踪筛选器，方法是指定应用此筛选器的 Storage Virtual Machine （SVM）名称以及此筛选器的索引编号。您可以修改所有可选筛选器参数。

步骤

1. 修改安全跟踪筛选器：

```
vserver security trace filter modify -vserver vserver_name -index  
index_number filter_parameters
```

- ° `vserver_name` 是要应用安全跟踪筛选器的SVM的名称。
- ° `index_number` 是要应用于筛选器的索引编号。此参数允许的值为 1 到 10 。
- ° `filter_parameters` 是可选筛选器参数的列表。

2. 验证安全跟踪筛选器条目：

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

示例

以下命令将使用索引编号 1 修改安全跟踪筛选器。筛选器可跟踪使用共享路径访问文件的任何用户的事件 \\server\share1\dir1\dir2\file.txt 从任何IP地址。筛选器将使用的完整路径 `-path` 选项筛选器跟踪允许和拒绝事件：

```
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
```

删除安全跟踪筛选器

如果不再需要安全跟踪筛选器条目，可以将其删除。由于每个 Storage Virtual Machine （

SVM) 最多可以有 10 个安全跟踪筛选器, 因此, 如果已达到最大值, 则可以通过删除不需要的筛选器来创建新筛选器。

关于此任务

要唯一标识要删除的安全跟踪筛选器, 必须指定以下内容:

- 应用跟踪筛选器的 SVM 的名称
- 跟踪筛选器的筛选器索引编号

步骤

1. 确定要删除的安全跟踪筛选器条目的筛选器索引编号:

```
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. 使用上一步中的筛选器索引编号信息删除筛选器条目:

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

3. 验证是否已删除安全跟踪筛选器条目:

```
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				

删除安全跟踪记录

在使用筛选器跟踪记录验证文件访问安全性或对 SMB 或 NFS 客户端访问问题进行故障排除后，您可以从安全跟踪日志中删除此安全跟踪记录。

关于此任务

在删除安全跟踪记录之前，您必须知道该记录的序列号。



每个 Storage Virtual Machine (SVM) 最多可存储 128 条跟踪记录。如果 SVM 上达到最大值，则添加新跟踪记录时，最早的跟踪记录将自动删除。如果您不想手动删除此 SVM 上的跟踪记录，可以让 ONTAP 在达到最大值后自动删除最旧的跟踪结果，以便为新结果腾出空间。

步骤

1. 确定要删除的记录的序列号：

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

2. 删除安全跟踪记录：

```
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 是发生要删除的权限跟踪事件的集群节点的名称。

这是必需的参数。

- ° -vserver vserver_name 是发生要删除的权限跟踪事件的SVM的名称。

这是必需的参数。

- ° -seqnum integer 是要删除的日志事件的序列号。

这是必需的参数。

删除所有安全跟踪记录

如果您不想保留任何现有安全跟踪记录，则只需使用一个命令即可删除节点上的所有记录。

步骤

1. 删除所有安全跟踪记录：

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

- `-node node_name` 是发生要删除的权限跟踪事件的集群节点的名称。
- `-vserver vserver_name` 是发生要删除的权限跟踪事件的Storage Virtual Machine (SVM)的名称。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。