執行安全追蹤
ONTAP 9

NetApp
April 24, 2024

目錄

執行安全追蹤

執行安全追蹤總覽

執行安全性追蹤包括建立安全性追蹤篩選器、驗證篩選條件、在符合篩選條件的SMB或NFS用戶端上產生存取要求、以及檢視結果。

完成使用安全篩選器擷取追蹤資訊之後、您可以修改篩選器並重複使用、或是在不再需要時停用篩選器。檢視及分析篩選追蹤結果之後、您可以在不再需要時將其刪除。

建立安全追蹤篩選器

您可以建立安全追蹤篩選器、以偵測儲存虛擬機器（SVM）上的SMB和NFS用戶端作業、並追蹤符合篩選器的所有存取檢查。您可以使用安全追蹤的結果來驗證組態或疑難排解存取問題。

關於這項工作

Vserver安全追蹤篩選器create命令需要兩個參數：

必要參數	說明
`-vserver vserver_name`	*SVM*名稱 包含您要套用安全性追蹤篩選器之檔案或資料夾的SVM名稱。
`-index index_number`	篩選索引編號_ 要套用至篩選的索引編號。每個SVM最多可有10個追蹤篩選器。此參數允許的值為1到10。

許多選用的篩選參數可讓您自訂安全性追蹤篩選器、以便縮小安全性追蹤所產生的結果：

篩選參數	說明
`-client-ip IP_Address`	此篩選器會指定使用者存取SVM的IP位址。
`-path path`	此篩選器會指定要套用權限追蹤篩選器的路徑。的價值 `-path` 可以使用下列其中一種格式： • 完整路徑、從共用區根目錄或匯出開始 • 部分路徑、相對於共用的根目錄 您必須在路徑值中使用NFS樣式目錄UNIX型目錄分隔符號。

`-windows-name win_user_name` 或 `-unix -name``unix_user_name`	您可以指定要追蹤其存取要求的Windows使用者名稱或UNIX使用者名稱。使用者名稱變數不區分大小寫。您無法在同一個篩選器中同時指定Windows使用者名稱和UNIX使用者名稱。 即使您可以追蹤SMB和NFS存取事件、對應的UNIX使用者和對應的UNIX使用者群組也可以在混合或UNIX安全型資料上執行存取檢查。
`-trace-allow {yes`	`no}`
安全性追蹤篩選器一律會啟用拒絕事件追蹤。您可以選擇追蹤允許事件。若要追蹤允許事件、請將此參數設為 `yes`。	`-enabled {enabled`
`disabled}`	您可以啟用或停用安全性追蹤篩選器。依預設、安全性追蹤篩選器為啟用狀態。
`-time-enabled integer`	您可以指定篩選器的逾時時間、之後篩選器就會停用。

步驟

1. 建立安全追蹤篩選器：

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

   `filter_parameters` 為選用篩選參數清單。

   如需詳細資訊、請參閱命令的手冊頁。

2. 驗證安全性追蹤篩選器項目：

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

範例

下列命令會為任何使用者建立安全性追蹤篩選器、以存取具有共用路徑的檔案 `\\server\share1\dir1\dir2\file.txt` 從 IP 位址 10.10.10.7 。篩選器使用的完整路徑 `-path` 選項。用於存取資料的用戶端IP位址為10.10.10.7.篩選器在30分鐘後逾時：

```
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       -
```

下列命令會使用的相對路徑來建立安全性追蹤篩選器 `-path` 選項。篩選器會追蹤名為「'joe'」之Windows使用者的存取權。Joe 正在存取具有共用路徑的檔案 `\\server\share1\dir1\dir2\file.txt`。篩選器追蹤會允許及拒絕事件：

```
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
```

顯示安全追蹤篩選器的相關資訊

您可以顯示儲存虛擬機器（SVM）上設定的安全追蹤篩選器相關資訊。這可讓您查看每個篩選器追蹤的存取事件類型。

步驟

1. 使用顯示安全性追蹤篩選項目的相關資訊 `vserver security trace filter show` 命令。

   如需使用此命令的詳細資訊、請參閱手冊頁。

範例

下列命令會顯示SVM VS1上所有安全追蹤篩選器的相關資訊：

```
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
```

顯示安全性追蹤結果

您可以顯示針對符合安全性追蹤篩選器的檔案作業所產生的安全性追蹤結果。您可以使用結果來驗證檔案存取安全性組態、或疑難排解SMB和NFS檔案存取問題。

您需要的產品

啟用的安全性追蹤篩選器必須存在、而且必須從SMB或NFS用戶端執行作業、且該用戶端必須符合安全性追蹤篩選器、才能產生安全性追蹤結果。

關於這項工作

您可以顯示所有安全性追蹤結果的摘要、也可以指定選用參數來自訂輸出中顯示的資訊。當安全性追蹤結果包含大量記錄時、這一點很有幫助。

如果您未指定任何選用參數、則會顯示下列項目：

- 儲存虛擬機器（SVM）名稱
- 節點名稱
- 安全性追蹤索引編號
- 安全風格
- 路徑
- 理由
- 使用者名稱

  使用者名稱會根據追蹤篩選器的設定方式顯示：

如果篩選器已設定…	然後…
使用UNIX使用者名稱	安全性追蹤結果會顯示UNIX使用者名稱。
使用Windows使用者名稱	安全性追蹤結果會顯示Windows使用者名稱。
沒有使用者名稱	安全性追蹤結果會顯示Windows使用者名稱。

您可以使用選用參數來自訂輸出。您可以使用某些選用參數來縮小命令輸出中傳回的結果範圍、其中包括：

選用參數	說明
`-fields field_name、 ...`	在您選擇的欄位上顯示輸出。您可以單獨使用此參數、也可以搭配其他選用參數一起使用。
`-instance`	顯示安全性追蹤事件的詳細資訊。此參數可搭配其他選用參數使用、以顯示特定篩選結果的詳細資訊。
`-node node_name`	僅顯示有關指定節點上事件的資訊。
`-vserver vserver_name`	僅顯示指定SVM上事件的相關資訊。
`-index integer`	顯示與指定索引編號對應之篩選器所產生之事件的相關資訊。
`-client-ip IP_address`	顯示從指定用戶端IP位址存取檔案所發生事件的相關資訊。
`-path path`	顯示因檔案存取指定路徑而發生事件的相關資訊。
`-user-name user_name`	顯示指定Windows或UNIX使用者存取檔案時所發生事件的相關資訊。
`-security-style security_style`	顯示在具有指定安全樣式的檔案系統上發生事件的相關資訊。

請參閱手冊頁、以取得可搭配命令使用的其他選用參數資訊。

步驟

1. 使用顯示安全性追蹤篩選結果 `vserver security trace trace-result show` 命令。

   `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/
   ```

修改安全性追蹤篩選器

如果您想要變更選用的篩選參數、以決定追蹤哪些存取事件、您可以修改現有的安全性追蹤篩選器。

關於這項工作

您必須指定要套用篩選器的儲存虛擬機器（SVM）名稱、以及篩選器的索引編號、以識別要修改的安全性追蹤篩選器。您可以修改所有選用的篩選參數。

步驟

1. 修改安全性追蹤篩選器：

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

   - `vserver_name` 是要套用安全性追蹤篩選器的 SVM 名稱。
   - `index_number` 是您要套用至篩選的索引編號。此參數允許的值為1到10。
   - `filter_parameters` 為選用篩選參數清單。

2. 驗證安全性追蹤篩選器項目：

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

範例

下列命令會修改索引編號為1的安全性追蹤篩選器。篩選器會追蹤任何使用者存取具有共用路徑之檔案的事件 `\\server\share1\dir1\dir2\file.txt` 來自任何 IP 位址。篩選器使用的完整路徑 `-path` 選項。篩選器追蹤會允許及拒絕事件：

```
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
```

刪除安全追蹤篩選器

當您不再需要安全性追蹤篩選器項目時、可以將其刪除。由於每個儲存虛擬機器（SVM）

最多可有10個安全追蹤篩選器、因此刪除不需要的篩選器後、您就能在達到上限時建立新的篩選器。

關於這項工作

若要唯一識別您要刪除的安全性追蹤篩選器、您必須指定下列項目：

- 套用追蹤篩選器的SVM名稱
- 追蹤篩選器的篩選索引編號

步驟

1. 識別您要刪除之安全性追蹤篩選器項目的篩選器索引編號：

   ```
   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. 使用上一個步驟的篩選索引編號資訊、刪除篩選項目：

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

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

3. 確認安全性追蹤篩選器項目已刪除：

   ```
   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
   ```

刪除安全性追蹤記錄

使用篩選器追蹤記錄來驗證檔案存取安全性或疑難排解SMB或NFS用戶端存取問題之後、您可以從安全性追蹤記錄中刪除安全性追蹤記錄。

關於這項工作

在刪除安全性追蹤記錄之前、您必須知道記錄的序號。

> 每個儲存虛擬機器（SVM）最多可儲存128筆追蹤記錄。如果SVM達到上限、則會在新增追蹤記錄時自動刪除最舊的追蹤記錄。如果您不想手動刪除此SVM上的追蹤記錄、ONTAP 可讓SVM在達到最大值後自動刪除最舊的追蹤結果、以便留出新結果的空間。

步驟

1. 識別您要刪除的記錄序號：

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

2. 刪除安全性追蹤記錄：

   ```
   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` 是您要刪除之權限追蹤事件所在的叢集節點名稱。

     這是必要的參數。

   - `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的 SVM 名稱。

     這是必要的參數。

   - `-seqnum integer` 為您要刪除的記錄事件序號。

     這是必要的參數。

刪除所有安全追蹤記錄

如果您不想保留任何現有的安全性追蹤記錄、可以使用單一命令刪除節點上的所有記錄。

步驟

1. 刪除所有安全追蹤記錄：

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

   - `-node node_name` 是您要刪除之權限追蹤事件所在的叢集節點名稱。

- `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的儲存虛擬機器（SVM）名稱。