보안 추적을 수행합니다

ONTAP 9

NetApp
February 12, 2026

목차

보안 추적을 수행합니다

ONTAP 보안 추적을 수행하는 방법을 알아보세요

보안 추적을 수행하려면 보안 추적 필터를 만들고, 필터 기준을 확인하고, 필터 기준과 일치하는 SMB 또는 NFS 클라이언트에 액세스 요청을 생성하고, 결과를 확인해야 합니다.

보안 필터를 사용하여 추적 정보를 캡처한 후 필터를 수정하고 다시 사용하거나 더 이상 필요하지 않은 경우 비활성화할 수 있습니다. 필터 추적 결과를 보고 분석한 후 더 이상 필요하지 않은 경우 삭제할 수 있습니다.

ONTAP SVM에서 보안 추적 필터 생성

SVM(스토리지 가상 머신)에서 SMB 및 NFS 클라이언트 작업을 감지하고 필터와 일치하는 모든 액세스 검사를 추적하는 보안 추적 필터를 생성할 수 있습니다. 보안 추적의 결과를 사용하여 구성을 확인하거나 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

vserver security trace filter create 명령에는 두 가지 필수 매개 변수가 있습니다.

필수 매개변수	설명
'-vserver"vserver_name'	_SVM 이름 _ 보안 추적 필터를 적용할 파일 또는 폴더가 포함된 SVM의 이름입니다.
인덱스 인덱스 인덱스 인덱스 번호	_필터 인덱스 번호 _ 필터에 적용할 인덱스 번호입니다. SVM당 최대 10개의 추적 필터로 제한됩니다. 이 매개 변수에 허용되는 값은 1 ~ 10입니다.

여러 선택적 필터 매개 변수를 사용하여 보안 추적 필터를 사용자 지정하여 보안 추적에서 생성된 결과를 좁힐 수 있습니다.

필터 매개 변수	설명
'-client-ip"ip_Address'	이 필터는 사용자가 SVM에 액세스하는 데 사용할 IP 주소를 지정합니다.
길의 길	이 필터는 권한 추적 필터를 적용할 경로를 지정합니다. '-path'의 값은 다음 형식 중 하나를 사용할 수 있습니다. • 공유 또는 내보내기의 루트에서 시작하는 전체 경로입니다 • 공유의 루트에 상대적인 부분 경로입니다 경로 값에 NFS 스타일 디렉토리 UNIX 스타일 디렉토리 구분 기호를 사용해야 합니다.

'-windows-name"win_user_name' 또는 '-unix-name"unix_user_name'	추적할 액세스 요청의 Windows 사용자 이름 또는 UNIX 사용자 이름을 지정할 수 있습니다. 사용자 이름 변수는 대/소문자를 구분하지 않습니다. 동일한 필터에 Windows 사용자 이름과 UNIX 사용자 이름을 모두 지정할 수는 없습니다. SMB 및 NFS 액세스 이벤트를 추적할 수 있더라도 UNIX 보안 스타일 데이터가 혼합된 데이터에 대한 액세스 검사를 수행할 때 매핑된 UNIX 사용자 및 매핑된 UNIX 사용자 그룹이 사용될 수 있습니다.
'-trace-allow'{'yes'	'no'}
거부 이벤트 추적은 항상 보안 추적 필터에 대해 활성화됩니다. 선택적으로 허용 이벤트를 추적할 수 있습니다. 허용 이벤트를 추적하려면 이 매개변수를 "예"로 설정합니다.	``사용'{'사용'
'사용 안 함'}	보안 추적 필터를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본적으로 보안 추적 필터는 활성화되어 있습니다.
시간 사용 정수	필터 시간 초과를 지정하면 필터 시간 초과가 해제됩니다.

단계

1. 보안 추적 필터 만들기:

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

   filter_parameters는 선택 필터 매개변수 목록입니다.

   에 대한 자세한 내용은 `vserver security trace filter create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 보안 추적 필터 항목을 확인합니다.

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

예

다음 명령을 실행하면 IP 주소 10.10.7에서 공유 경로 '\\server\share1\dir1\dir2\file.txt'를 사용하여 파일에 액세스하는 모든 사용자에 대한 보안 추적 필터가 생성됩니다. 이 필터는 '-path' 옵션을 위한 전체 경로를 사용합니다. 데이터에 액세스하는 데 사용되는 클라이언트의 IP 주소는 10.10.7입니다. 필터는 30분 후에 시간 초과됩니다.

```
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       -
```

다음 명령을 실행하면 '-path' 옵션에 대한 상대 경로를 사용하여 보안 추적 필터를 만듭니다. 이 필터는 ""Joe""라는 이름의 Windows 사용자에 대한 액세스를 추적합니다. Joe가 공유 경로 '\\server\share1\dir1\dir2\file.txt'를 사용하여 파일에 액세스하고 있습니다. 필터 추적은 이벤트를 허용 및 거부합니다.

```
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
```

ONTAP SVM의 보안 추적 필터에 대한 정보 표시

SVM(스토리지 가상 시스템)에 구성된 보안 추적 필터에 대한 정보를 표시할 수 있습니다. 이를 통해 각 필터 추적의 액세스 이벤트 유형을 확인할 수 있습니다.

단계

1. 'vserver security trace filter show' 명령을 사용하여 보안 추적 필터 항목에 대한 정보를 출력한다.

   에 대한 자세한 내용은 `vserver security trace filter show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령을 실행하면 SVM VS1 의 모든 보안 추적 필터에 대한 정보가 표시됩니다.

```
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
```

ONTAP SVM에서 보안 추적 결과 표시

보안 추적 필터와 일치하는 파일 작업에 대해 생성된 보안 추적 결과를 표시할 수 있습니다. 이 결과를 사용하여 파일 액세스 보안 구성을 검증하거나 SMB 및 NFS 파일 액세스 문제를 해결할 수 있습니다.

시작하기 전에

활성화된 보안 추적 필터가 있어야 하며 보안 추적 결과를 생성하려면 보안 추적 필터와 일치하는 SMB 또는 NFS 클라이언트에서 작업을 수행해야 합니다.

이 작업에 대해

모든 보안 추적 결과의 요약을 표시하거나 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다. 이 기능은 보안 추적 결과에 많은 수의 레코드가 포함된 경우에 유용합니다.

선택적 매개 변수를 지정하지 않으면 다음 항목이 표시됩니다.

- 스토리지 가상 시스템(SVM) 이름
- 노드 이름
- Security Trace Index Number이다
- 보안 스타일
- 경로
- 이유
- 사용자 이름입니다

  추적 필터 구성 방법에 따라 사용자 이름이 표시됩니다.

필터가 구성된 경우…	그러면…
UNIX 사용자 이름을 사용합니다	보안 추적 결과에 UNIX 사용자 이름이 표시됩니다.
Windows 사용자 이름을 사용합니다	보안 추적 결과에 Windows 사용자 이름이 표시됩니다.
사용자 이름이 없습니다	보안 추적 결과에 Windows 사용자 이름이 표시됩니다.

선택적 매개 변수를 사용하여 출력을 사용자 지정할 수 있습니다. 명령 출력에 반환되는 결과의 범위를 좁히는 데 사용할 수 있는 선택적 매개 변수 중 몇 가지는 다음과 같습니다.

선택적 매개 변수입니다	설명
``필드''필드_이름, …	선택한 필드에 출력을 표시합니다. 이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.
'-인스턴스'	보안 추적 이벤트에 대한 자세한 정보를 표시합니다. 이 매개 변수를 다른 선택적 매개 변수와 함께 사용하면 특정 필터 결과에 대한 자세한 정보를 표시할 수 있습니다.
'-node' node_name'입니다	지정된 노드의 이벤트에 대한 정보만 표시합니다.
'-vserver"vserver_name'	지정된 SVM의 이벤트에 대한 정보만 표시합니다.
인덱스 정수	지정된 인덱스 번호에 해당하는 필터의 결과로 발생한 이벤트에 대한 정보를 표시합니다.
'-client-ip"ip_address'	지정된 클라이언트 IP 주소에서 파일 액세스로 인해 발생한 이벤트에 대한 정보를 표시합니다.
길의 길	지정된 경로에 대한 파일 액세스 결과로 발생한 이벤트에 대한 정보를 표시합니다.
'-user-name"user_name'입니다	지정된 Windows 또는 UNIX 사용자가 파일에 액세스한 결과로 발생한 이벤트에 대한 정보를 표시합니다.
'-security-style"security_style'	지정된 보안 스타일이 있는 파일 시스템에서 발생한 이벤트에 대한 정보를 표시합니다.

기타 선택적 매개 변수에 대한 자세한 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 'vserver security trace trace trace -result show' 명령어를 사용해 보안추적 필터 결과를 출력한다.

   'vserver security trace trace-result show-user-name domain\user'를 선택합니다

```
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/
```

ONTAP SVM에서 보안 추적 필터 수정

추적할 액세스 이벤트를 결정하는 데 사용되는 선택적 필터 매개 변수를 변경하려면 기존 보안 추적 필터를 수정할 수 있습니다.

이 작업에 대해

필터가 적용되는 SVM(Storage Virtual Machine) 이름과 필터의 인덱스 번호를 지정하여 수정할 보안 추적 필터를 식별해야 합니다. 모든 선택적 필터 매개 변수를 수정할 수 있습니다.

단계

1. 보안 추적 필터 수정:

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

   - vserver_name은 보안 추적 필터를 적용할 SVM의 이름입니다.
   - index_number는 필터에 적용할 인덱스 번호입니다. 이 매개 변수에 허용되는 값은 1 ~ 10입니다.
   - filter_parameters는 선택 필터 매개변수 목록입니다.
2. 보안 추적 필터 항목을 확인합니다.

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

예

다음 명령을 실행하면 인덱스 번호 1로 보안 추적 필터가 수정됩니다. 이 필터는 IP 주소에서 공유 경로 '\\server\share1\dir1\dir2\file.txt'를 사용하여 파일에 액세스하는 모든 사용자에 대한 이벤트를 추적합니다. 이 필터는 '-path' 옵션을 위한 전체 경로를 사용합니다. 필터 추적은 이벤트를 허용 및 거부합니다.

```
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
```

ONTAP SVM에서 보안 추적 필터 삭제

보안 추적 필터 항목이 더 이상 필요하지 않으면 삭제할 수 있습니다. SVM(스토리지 가상 시스템)당 최대 10개의 보안 추적 필터를 사용할 수 있으므로 불필요한 필터를 삭제하면 최대 한도까지 도달했을 때 새 필터를 생성할 수 있습니다.

이 작업에 대해

삭제할 보안 추적 필터를 고유하게 식별하려면 다음을 지정해야 합니다.

- 트레이스 필터가 적용된 SVM의 이름입니다
- 추적 필터의 필터 인덱스 번호입니다

단계

1. 삭제할 보안 추적 필터 항목의 필터 인덱스 번호를 식별합니다.

   'vserver security trace filter show -vserver vserver_name'

   'vserver security trace filter show -vserver vs1'이 표시됩니다

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. 이전 단계의 필터 인덱스 번호 정보를 사용하여 필터 항목을 삭제합니다.

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

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

3. 보안 추적 필터 항목이 삭제되었는지 확인합니다.

   'vserver security trace filter show -vserver vserver_name'

   'vserver security trace filter show -vserver vs1'이 표시됩니다

```
Vserver  Index   Client-IP            Path             Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

ONTAP SVM에서 보안 추적 레코드 삭제

필터 추적 레코드를 사용하여 파일 액세스 보안을 확인하거나 SMB 또는 NFS 클라이언트 액세스 문제를 해결하면 보안 추적 로그에서 보안 추적 레코드를 삭제할 수 있습니다.

이 작업에 대해

보안 추적 레코드를 삭제하려면 먼저 레코드의 시퀀스 번호를 알아야 합니다.

> 각 SVM(스토리지 가상 머신)에는 최대 128개의 추적 레코드를 저장할 수 있습니다. SVM에서 최대값을 선택하면 새 트레이스 레코드가 추가될 때 가장 오래된 트레이스 레코드가 자동으로 삭제됩니다. 이 SVM에서 트레이스 레코드를 수동으로 삭제하지 않을 경우 최대 한도에 도달한 후 ONTAP에서 가장 오래된 트레이스 결과를 자동으로 삭제하여 새 결과를 얻을 수 있는 공간을 만들 수 있습니다.

단계

1. 삭제할 레코드의 시퀀스 번호를 식별합니다.

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

2. 보안 추적 레코드를 삭제합니다.

   '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'은 삭제하려는 권한 추적 이벤트가 발생한 클러스터 노드의 이름입니다.

     필수 매개 변수입니다.

   - '-vserver"vserver_name'은 삭제할 권한 추적 이벤트가 발생한 SVM의 이름입니다.

     필수 매개 변수입니다.

   - '-seqnum' 정수 는 삭제하려는 로그 이벤트의 시퀀스 번호입니다.

필수 매개 변수입니다.

ONTAP SVM의 모든 보안 추적 레코드 삭제

기존 보안 추적 레코드를 유지하지 않으려면 한 번의 명령으로 노드의 모든 레코드를 삭제할 수 있습니다.

단계

1. 모든 보안 추적 레코드 삭제:

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

   - '-node "node_name'은 삭제하려는 권한 추적 이벤트가 발생한 클러스터 노드의 이름입니다.
   - '-vserver"vserver_name'은 삭제할 권한 추적 이벤트가 발생한 SVM(스토리지 가상 시스템)의 이름입니다.