# NFS 지원 SVM에 스토리지 용량 추가

ONTAP 9

NetApp
May 09, 2024

# 목차

# NFS 지원 SVM에 스토리지 용량 추가

## NFS 지원 SVM 개요에 스토리지 용량을 추가합니다

NFS 지원 SVM에 스토리지 용량을 추가하려면 스토리지 컨테이너를 제공할 볼륨 또는 qtree를 생성하고 해당 컨테이너의 엑스포트 정책을 생성하거나 수정해야 합니다. 그런 다음 클러스터에서 NFS 클라이언트 액세스를 확인하고 클라이언트 시스템에서 액세스를 테스트할 수 있습니다.

필요한 것

- SVM에서 NFS를 완전히 설정해야 합니다.
- SVM 루트 볼륨의 기본 엑스포트 정책에는 모든 클라이언트에 액세스할 수 있는 규칙이 포함되어 있어야 합니다.
- 이름 서비스 구성에 대한 모든 업데이트를 완료해야 합니다.
- Kerberos 구성에 대한 추가 또는 수정을 완료해야 합니다.

## 엑스포트 정책을 생성합니다

내보내기 규칙을 만들기 전에 해당 규칙을 보유할 내보내기 정책을 만들어야 합니다. 'vserver export-policy create' 명령을 사용하여 엑스포트 정책을 생성할 수 있습니다.

단계

1. 엑스포트 정책 생성:

   'vserver export-policy create-vserver_vserver_name_-policyname_policy_name_'

   정책 이름은 최대 256자까지 지정할 수 있습니다.

2. 엑스포트 정책이 생성되었는지 확인:

   'vserver export-policy show-policyname_policy_name_'

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 exp1 이라는 엑스포트 정책이 생성되는지 검증 및 됩니다.

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

# 엑스포트 정책에 규칙 추가

규칙이 없으면 내보내기 정책은 클라이언트에 데이터에 대한 액세스를 제공할 수 없습니다. 새 내보내기 규칙을 만들려면 클라이언트를 식별하고 클라이언트 일치 형식을 선택하고, 액세스 및 보안 유형을 선택하고, 익명 사용자 ID 매핑을 지정하고, 규칙 인덱스 번호를 선택하고, 액세스 프로토콜을 선택해야 합니다. 그런 다음 'vserver export-policy rule create' 명령을 사용하여 내보내기 정책에 새 규칙을 추가할 수 있습니다.

필요한 것

- 내보내기 규칙을 추가할 엑스포트 정책이 이미 있어야 합니다.
- 데이터 SVM에서 DNS를 올바르게 구성해야 하며, DNS 서버는 NFS 클라이언트를 위한 올바른 항목을 가지고 있어야 합니다.

  이는 ONTAP가 특정 클라이언트 일치 형식에 대해 데이터 SVM의 DNS 구성을 사용하여 DNS 조회를 수행하고, 엑스포트 정책 규칙 일치의 실패로 인해 클라이언트 데이터 액세스가 차단되기 때문입니다.

- Kerberos를 사용하여 인증하는 경우 NFS 클라이언트에서 사용되는 다음 보안 방법 중 하나를 결정해야 합니다.
  - "krb5"(Kerberos V5 프로토콜)
  - "krb5i"(체크섬을 사용한 무결성 검사가 가능한 Kerberos V5 프로토콜)
  - 'krb5p'(개인정보 보호 서비스가 있는 Kerberos V5 프로토콜)

이 작업에 대해

내보내기 정책의 기존 규칙이 클라이언트 일치 및 액세스 요구 사항을 포함하는 경우에는 새 규칙을 생성할 필요가 없습니다.

Kerberos를 사용하여 인증하는 경우 Kerberos를 통해 SVM의 모든 볼륨에 액세스할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5', krb5i 또는 krb5p로 설정할 수 있습니다.

단계

1. 새 규칙의 클라이언트 및 클라이언트 일치 형식을 식별합니다.

   '-clientmatch' 옵션은 규칙이 적용되는 클라이언트를 지정합니다. 하나 또는 여러 개의 클라이언트 일치 값을 지정할 수 있습니다. 여러 값의 사양은 쉼표로 구분해야 합니다. 다음 형식 중 하나로 일치 항목을 지정할 수 있습니다.

| 클라이언트 일치 형식입니다 | 예 |
|---|---|
| 도메인 이름 앞에 "." 문자가 옵니다 | |
| 호스트 이름입니다 | 'host1' 또는 'host1, host2,...' |
| IPv4 주소입니다 | 10.1.12.24 또는 + 10.1.12.24,10.1.12.25,…+ |
| 서브넷 마스크가 있는 IPv4 주소는 비트 수로 표시됩니다 | 10.1.12.10/4, 또는 + 10.1.12.10/4,10.1.12.11/4,…+ |

| 클라이언트 일치 형식입니다 | 예 |
|---|---|
| 네트워크 마스크가 있는 IPv4 주소입니다 | 10.1.16.0/255.255.255.0 또는 + 10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0,…+ |
| 점선 형식의 IPv6 주소입니다 | '::1.2.3.4' 또는 '::1.2.3.4,::1.2.3.5,...' |
| 서브넷 마스크가 있는 IPv6 주소는 비트 수로 표시됩니다 | "ff::00/32" 또는 "ff::00/32, ff: 01/32,..." |
| 넷그룹 이름 앞에 @ 문자가 오는 단일 넷그룹 | '@netgroup1' 또는 '@netgroup1,@netgroup2,...' |

클라이언트 정의 형식(예: '.example.com,@netgroup1`)을 결합할 수도 있습니다.

IP 주소를 지정할 때 다음 사항에 유의하십시오.

- 10.1.12.10-10.1.12.70 등의 IP 주소 범위를 입력할 수 없습니다.

  이 형식의 항목은 텍스트 문자열로 해석되며 호스트 이름으로 처리됩니다.

- 클라이언트 액세스의 세부 관리에 대한 내보내기 규칙에서 개별 IP 주소를 지정할 때 동적으로 할당되는 IP 주소(예: DHCP) 또는 임시로 할당된 IP 주소(예: IPv6)를 지정하지 마십시오.

  그렇지 않으면 IP 주소가 변경되면 클라이언트가 액세스 권한을 잃게 됩니다.

- 네트워크 마스크로 IPv6 주소(예: ff::12/ff::00)를 입력할 수 없습니다.

2. 클라이언트 일치에 대한 액세스 및 보안 유형을 선택합니다.

   지정된 보안 유형으로 인증하는 클라이언트에 대해 다음 액세스 모드 중 하나 이상을 지정할 수 있습니다.

   - '-rorule'(읽기 전용 액세스)
   - '-rwrule'(읽기-쓰기 액세스)
   - '-superuser'(루트 액세스)

   > 내보내기 규칙에서 해당 보안 유형에 대한 읽기 전용 액세스도 허용하는 경우 클라이언트는 특정 보안 유형에 대한 읽기-쓰기 액세스만 얻을 수 있습니다. 읽기 전용 매개 변수가 읽기-쓰기 매개 변수보다 보안 형식에 대해 더 제한적인 경우 클라이언트는 읽기-쓰기 액세스를 얻지 못할 수 있습니다. 수퍼유저 액세스도 마찬가지입니다.

   규칙에 대해 여러 보안 유형의 쉼표로 구분된 목록을 지정할 수 있습니다. 보안 유형을 "모두" 또는 "사용 안 함"으로 지정하는 경우 다른 보안 유형을 지정하지 마십시오. 다음 유효한 보안 유형 중에서 선택하십시오.

| 보안 유형을 다음으로 설정한 경우… | 일치하는 클라이언트가 내보낸 데이터에 액세스할 수 있습니다… |
|---|---|
| 모두 | 항상, 들어오는 보안 유형에 관계없이. |

| 보안 유형을 다음으로 설정한 경우... | 일치하는 클라이언트가 내보낸 데이터에 액세스할 수 있습니다... |
|---|---|
| "없음" | 보안 유형을 가진 클라이언트만 나열되면 익명 액세스 권한이 부여됩니다. 다른 보안 유형과 함께 나열되는 경우 지정된 보안 유형의 클라이언트는 액세스 권한이 부여되고 다른 보안 유형의 클라이언트는 익명 액세스 권한이 부여됩니다. |
| "안 돼. | 수신 보안 유형에 관계없이 사용 안 함. |
| krb5 | Kerberos 5에 의해 인증되는 경우 인증 전용: 각 요청 및 응답의 헤더가 서명됩니다. |
| krb5i | Kerberos 5i에 의해 인증되는 경우. 인증 및 무결성: 각 요청 및 응답의 헤더와 본문이 서명됩니다. |
| 크르b5p | Kerberos 5p에 의해 인증되는 경우 인증, 무결성 및 개인 정보 보호: 각 요청 및 응답의 헤더와 본문이 서명되고 NFS 데이터 페이로드가 암호화됩니다. |
| NTLM | CIFS NTLM에 의해 인증되는 경우 |
| '스'입니다 | NFS AUTH_SYS에 의해 인증되는 경우 |

권장 보안 유형은 '시스', 또는 Kerberos를 사용하는 경우 krb5, krb5i, krb5p입니다.

NFSv3에서 Kerberos를 사용하는 경우, 내보내기 정책 규칙은 krb5 이외에 '-rorule' 및 '-rwrule' 액세스를 허용해야 합니다. 이는 내보내기에 대한 NLM(Network Lock Manager) 액세스를 허용해야 하기 때문입니다.

3. 익명 사용자 ID 매핑을 지정합니다.

   '-anon' 옵션은 사용자 ID가 0인 클라이언트 요청에 매핑된 UNIX 사용자 ID 또는 사용자 이름을 지정합니다. 이 사용자 이름은 일반적으로 사용자 이름 루트와 연결됩니다. 기본값은 65534입니다. NFS 클라이언트는 일반적으로 사용자 ID 65534를 사용자 이름 nobody(또는 *root squooting*)와 연결합니다. ONTAP에서 이 사용자 ID는 사용자 pcuser와 연결됩니다. 사용자 ID가 0인 클라이언트에서 액세스를 비활성화하려면 값을 65535로 지정합니다.

4. 규칙 인덱스 순서를 선택합니다.

   ruleindex 옵션은 규칙의 인덱스 번호를 지정합니다. 규칙은 인덱스 번호 목록의 순서에 따라 평가되며, 인덱스 번호가 낮은 규칙은 먼저 평가됩니다. 예를 들어 인덱스 번호가 1인 규칙은 인덱스 번호가 2인 규칙 전에 평가됩니다.

| 추가하는 경우... | 그러면... |
|---|---|
| 엑스포트 정책에 대한 첫 번째 규칙 | 1을 입력합니다. |

| 추가하는 경우... | 그러면... |
| --- | --- |
| 엑스포트 정책에 대한 추가 규칙 | a. 정책에 기존 규칙을 표시합니다. + 'vserver export-policy rule show-instance-policyname_your_policy_'<br>b. 평가해야 하는 순서에 따라 새 규칙의 인덱스 번호를 선택합니다. |

5. 해당 NFS 액세스 값 {'NFS'|'NFS3'|'nfs4'}을 선택합니다.

   NFS는 어떤 버전이든 일치하며 NFS3, nfs4는 특정 버전만을 일치시킵니다.

6. 내보내기 규칙을 만들어 기존 엑스포트 정책에 추가합니다.

   'vserver export-policy rule create-vserver_vserver_name_-policyname_policy_name_-ruleindex_integer_-protocol{nNFS|NFS3|nfs4}-clientmatch {text|*"text,text,…"*}-rorule_security_type_-superuser_security_type_ananID

7. 내보내기 정책의 규칙을 표시하여 새 규칙이 있는지 확인합니다.

   'vserver export-policy rule show-policyname_policy_name_'

   명령은 해당 정책에 적용되는 규칙 목록을 포함하여 해당 엑스포트 정책에 대한 요약을 표시합니다. ONTAP는 각 규칙에 규칙 인덱스 번호를 할당합니다. 규칙 인덱스 번호를 알고 나면 이 번호를 사용하여 지정된 엑스포트 규칙에 대한 자세한 정보를 표시할 수 있습니다.

8. 내보내기 정책에 적용된 규칙이 올바르게 구성되었는지 확인합니다.

   'vserver export-policy rule show -policyname_policy_name_-vserver_vserver_name_-ruleindex_integer_'

예

다음 명령은 RS1이라는 엑스포트 정책에서 VS1이라는 SVM에 엑스포트 규칙이 생성되었는지 확인합니다. 규칙에 인덱스 번호가 1입니다. 이 규칙은 eng.company.com 도메인에 있는 모든 클라이언트와 netgroup@netgroup1과 일치합니다. 이 규칙은 모든 NFS 액세스를 설정합니다. AUTH_SYS로 인증된 사용자에 대한 읽기 전용 및 읽기-쓰기 액세스를 활성화합니다. UNIX 사용자 ID가 0인 클라이언트는 Kerberos로 인증되지 않는 한 익명화됩니다.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                               @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                     Vserver: vs1
                                 Policy Name: exp1
                                  Rule Index: 1
                             Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                              RO Access Rule: sys
                              RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: krb5
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

다음 명령은 expol2라는 엑스포트 정책에서 VS2라는 SVM에 엑스포트 규칙이 생성되었는지 확인합니다. 규칙의 인덱스 번호는 21입니다. 이 규칙은 클라이언트를 netgroup dev_netgroup_main의 구성원과 일치시킵니다. 이 규칙은 모든 NFS 액세스를 설정합니다. AUTH_SYS로 인증되고 읽기-쓰기 및 루트 액세스에 Kerberos 인증이 필요한 사용자에 대해 읽기 전용 액세스를 활성화합니다. UNIX 사용자 ID가 0인 클라이언트는 Kerberos로 인증되지 않는 한 루트 액세스가 거부됩니다.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                   Vserver: vs2
                               Policy Name: expol2
                                Rule Index: 21
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

# 볼륨 또는 qtree 스토리지 컨테이너를 생성합니다

## 볼륨을 생성합니다

볼륨을 생성하고 "volume create" 명령을 사용하여 해당 접합 지점 및 기타 속성을 지정할 수 있습니다.

### 이 작업에 대해

클라이언트에서 데이터를 사용할 수 있도록 하려면 볼륨에 _junction path_가 포함되어야 합니다. 새 볼륨을 생성할 때 접합 경로를 지정할 수 있습니다. 접합 경로를 지정하지 않고 볼륨을 생성하는 경우, "volume mount" 명령을 사용하여 SVM 네임스페이스에서 볼륨을 _mount_해야 합니다.

### 시작하기 전에

- NFS를 설정하고 실행해야 합니다.
- SVM 보안 유형은 UNIX여야 합니다.
- ONTAP 9.13.1 부터는 용량 분석 및 활동 추적 기능이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 을 실행합니다 `volume create` 명령을 사용합니다 `-analytics-state` 또는 `-activity`

`-tracking-state` 를 로 설정합니다 `on`.

용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 파일 시스템 분석 설정.

단계

1. 교차점으로 볼륨을 생성합니다.

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   '-junction-path'의 선택 항목은 다음과 같습니다.

   - 루트 바로 아래, 예: '/*new_vol*'

     새 볼륨을 생성하고 SVM 루트 볼륨에 직접 마운트하도록 지정할 수 있습니다.

   - 기존 디렉토리 아래에, 예: "/*existing_dir/new_vol*"

     새 볼륨을 생성하고 기존 계층 구조에서 기존 볼륨에 마운트하도록 지정할 수 있습니다. 이 볼륨은 디렉토리로 표시됩니다.

     새 볼륨 아래의 새 계층 구조에서 "*/new_dir/new_vol*"와 같은 새 디렉토리에 볼륨을 생성하려면 먼저 SVM 루트 볼륨에 대한 분기인 새 상위 볼륨을 생성해야 합니다. 그런 다음 새 상위 볼륨(새 디렉토리)의 접합 경로에 새 하위 볼륨을 생성합니다.

   + 기존 엑스포트 정책을 사용하려는 경우 볼륨을 생성할 때 지정할 수 있습니다. 나중에 볼륨 수정 명령을 사용하여 내보내기 정책을 추가할 수도 있습니다.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

예

다음 명령을 실행하면 SVM vs1.example.com 및 애그리게이트 aggr1에 user1이라는 새 볼륨이 생성됩니다. 새 볼륨은 '/users'에서 사용할 수 있습니다. 볼륨의 크기는 750GB이고 볼륨 유형은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

다음 명령을 실행하면 SVM "vs1.example.com" 및 애그리게이트 "aggr1"에 "home4"라는 새 볼륨이 생성됩니다. VS1

SVM은 이름 공간에 /ENG/ 디렉토리가 이미 있으며, '/ENG/' 네임스페이스의 홈 디렉토리가 되는 '/ENG/HOME'에서 새 볼륨을 사용할 수 있습니다. 볼륨 크기는 750GB이고 볼륨 보장은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

## qtree를 생성합니다

### 'volume qtree create' 명령을 사용하여 데이터를 포함하는 qtree를 생성하고 해당 속성을 지정할 수 있습니다.

필요한 것

- SVM과 새 qtree가 포함될 볼륨이 이미 존재해야 합니다.
- SVM 보안 스타일은 UNIX여야 하며 NFS를 설정하고 실행해야 합니다.

단계

1. qtree 생성:

   '볼륨 qtree create-vserver_vserver_name_{-volume_volume_name_-qtree_qtree_name_|-qtree-path_qtree path_} - 보안 스타일 UNIX [-policy_export_policy_name_]'

   볼륨과 qtree를 별도의 인수로 지정하거나 qtree 경로 인수를 '/vol/*volume_name/_qtree_name*' 형식으로 지정할 수 있습니다.

   기본적으로 Qtree는 상위 볼륨의 엑스포트 정책을 상속하지만, 자체 정책을 사용하도록 구성할 수 있습니다. 기존 엑스포트 정책을 사용하려는 경우 qtree를 생성할 때 지정할 수 있습니다. 나중에 'volume qtree modify' 명령을 사용하여 엑스포트 정책을 추가할 수도 있습니다.

2. qtree가 원하는 접합 경로로 생성되었는지 확인합니다.

   'volume qtree show-vserver_vserver_name_{-volume_volume_name_-qtree_qtree_name_|-qtree-path_qtree path_}'

예

다음 예에서는 junction path '/vol/data1'이 있는 SVM vs1.example.com 에 qt01이라는 이름의 qtree를 생성합니다.

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                   Security Style: unix
                      Oplock Mode: enable
                 Unix Permissions: ---rwxr-xr-x
                         Qtree Id: 2
                     Qtree Status: normal
                    Export Policy: default
        Is Export Policy Inherited: true
```

# 내보내기 정책을 사용하여 **NFS** 액세스를 보호합니다

## 내보내기 정책을 사용하여 **NFS** 액세스를 보호합니다

엑스포트 정책을 사용하여 볼륨 또는 qtree에 대한 NFS 액세스를 특정 매개 변수와 일치하는 클라이언트로 제한할 수 있습니다. 새 스토리지를 프로비저닝할 때 기존 정책 및 규칙을 사용하거나, 기존 정책에 규칙을 추가하거나, 새 정책 및 규칙을 생성할 수 있습니다. 내보내기 정책의 구성을 확인할 수도 있습니다

> ONTAP 9.3부터 오류 규칙 목록에 규칙 위반을 기록하는 백그라운드 작업으로 내보내기 정책 구성 검사를 활성화할 수 있습니다. 'vserver export-policy config-checker' 명령은 checker를 호출하여 결과를 표시합니다. 이 명령을 사용하면 구성을 확인하고 정책에서 잘못된 규칙을 삭제할 수 있습니다. 명령은 호스트 이름, 넷그룹 및 익명 사용자에 대한 내보내기 구성만 검증합니다.

## 내보내기 규칙의 처리 순서를 관리합니다

'vserver export-policy rule setindex' 명령을 사용하여 기존 엑스포트 규칙의 인덱스 번호를 수동으로 설정할 수 있습니다. 이렇게 하면 ONTAP가 클라이언트 요청에 내보내기 규칙을 적용하는 우선 순위를 지정할 수 있습니다.

이 작업에 대해

새 인덱스 번호가 이미 사용 중인 경우 명령은 지정된 위치에 규칙을 삽입하고 이에 따라 목록의 순서를 다시 지정합니다.

단계

1. 지정된 엑스포트 규칙의 인덱스 번호 수정:

   'vserver export-policy rule setindex-vserver_virtual_server_name_-policyname_policy_name_-ruleindex_integer_-newruleindex_integer_'

예

다음 명령을 실행하면 VS1 이라는 SVM의 RS1 엑스포트 정책에서 인덱스 번호 3에 있는 엑스포트 규칙의 인덱스 번호가 인덱스 번호 2로 변경됩니다.

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

## 볼륨에 엑스포트 정책을 할당합니다

## SVM에 포함된 각 볼륨은 클라이언트의 볼륨 데이터 액세스 엑스포트 규칙이 포함된 엑스포트 정책과 연결되어야 합니다.

이 작업에 대해

볼륨을 생성할 때 또는 볼륨을 생성한 후 언제든지 엑스포트 정책을 볼륨에 연결할 수 있습니다. 하나의 정책을 여러 볼륨에 연결할 수 있지만 하나의 엑스포트 정책을 볼륨에 연결할 수 있습니다.

단계

1. 볼륨을 생성할 때 엑스포트 정책을 지정하지 않은 경우 볼륨에 엑스포트 정책을 할당합니다.

   'volume modify -vserver_vserver_name_-volume_volume_name_-policy_export_policy_name_'

2. 정책이 볼륨에 할당되었는지 확인합니다.

   'volume show-volume_volume_name_-fields policy'입니다

예

다음 명령은 SVM VS1 볼륨 vol1에 엑스포트 정책 NFS_policy를 할당하고 할당을 확인합니다.

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

## qtree에 엑스포트 정책을 할당합니다

## 전체 볼륨을 내보내는 대신, 볼륨에 있는 특정 qtree를 엑스포트하여 클라이언트에서 직접 액세스할 수도 있습니다. 엑스포트 정책을 qtree에 할당하여 qtree를 내보낼 수 있습니다. 새 qtree를 생성하거나 기존 qtree를 수정하여 엑스포트 정책을 할당할 수 있습니다.

필요한 것

엑스포트 정책이 있어야 합니다.

이 작업에 대해

기본적으로 Qtree는 생성 시 별도로 지정하지 않을 경우 포함하는 볼륨의 상위 엑스포트 정책을 상속합니다.

qtree를 생성하거나 qtree를 생성한 후 언제든지 엑스포트 정책을 qtree에 연결할 수 있습니다. 하나의 정책을 여러 qtree와 연결할 수 있지만 하나의 엑스포트 정책을 qtree에 연결할 수 있습니다.

단계

1. Qtree 생성 시 엑스포트 정책을 지정하지 않은 경우 qtree에 엑스포트 정책을 할당하십시오.

   '볼륨 qtree modify -vserver_vserver_name_-qtree -path /vol/*volume_name /qtree_name*-export -policy_export_policy_name_'

2. 정책이 qtree에 할당되었는지 확인합니다.

   'volume qtree show-qtree_qtree_name_-fields export-policy'

예

다음 명령은 SVM VS1 의 qtree q1에 엑스포트 정책 NFS_policy를 할당하고 할당을 확인합니다.

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

# 클러스터에서 **NFS** 클라이언트 액세스를 확인합니다

UNIX 관리 호스트에서 UNIX 파일 권한을 설정하여 선택한 클라이언트에 공유에 대한 액세스 권한을 부여할 수 있습니다. 'vserver export-policy check-access' 명령을 사용하여 필요에 따라 내보내기 규칙을 조정하여 클라이언트 액세스를 확인할 수 있습니다.

단계

1. 클러스터에서 'vserver export-policy check-access' 명령을 사용하여 내보내기에 대한 클라이언트 액세스를 확인합니다.

   다음 명령은 IP 주소 1.2.4를 사용하여 볼륨 home2에 대한 NFSv3 클라이언트의 읽기/쓰기 액세스를 확인합니다. 명령 출력에서는 볼륨이 내보내기 정책 'exp-home-dir'을 사용하고 액세스가 거부됨을 보여 줍니다.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                          Policy    Policy     Rule
Path                      Policy          Owner     Owner Type Index  Access
------------------------ ------------- --------- ---------- ------
----------
/                         default       vs1_root  volume          1 read
/eng                      default       vs1_root  volume          1 read
/eng/home2                exp-home-dir  home2     volume          1 denied

3 entries were displayed.
```

2. 출력을 검사하여 내보내기 정책이 의도한 대로 작동하고 클라이언트 액세스가 예상대로 작동하는지 확인합니다.

   특히, 볼륨 또는 qtree에서 사용하는 엑스포트 정책과 이로 인해 클라이언트가 사용하는 액세스 유형을 확인해야 합니다.

3. 필요한 경우 엑스포트 정책 규칙을 다시 구성하십시오.

# 클라이언트 시스템에서 **NFS** 액세스를 테스트합니다

새 스토리지 개체에 대한 NFS 액세스를 검증한 후 NFS 관리 호스트에 로그인하고 SVM에서 데이터를 읽고 쓰는 방법으로 구성을 테스트해야 합니다. 그런 다음 클라이언트 시스템에서 루트 이외의 사용자로 프로세스를 반복해야 합니다.

필요한 것

- 클라이언트 시스템에는 이전에 지정한 내보내기 규칙에서 허용하는 IP 주소가 있어야 합니다.
- 루트 사용자에 대한 로그인 정보가 있어야 합니다.

단계

1. 클러스터에서 새 볼륨을 호스팅하는 LIF의 IP 주소를 확인합니다.

   'network interface show –vserver_svm_name_'

2. 관리 호스트 클라이언트 시스템에 루트 사용자로 로그인합니다.
3. 디렉토리를 마운트 폴더로 변경합니다.

   "cd /mnt/"

4. SVM의 IP 주소를 사용하여 새 폴더를 생성하고 마운트합니다.

   a. 새 폴더: + mkdir /mnt/*folder'*를 만듭니다
   b. 이 새 디렉토리에 새 볼륨을 마운트합니다. + mount -t nfs -o hard_IPAddress_:/*volume_name*/mnt/*folder'*
   c. 디렉터리를 새 폴더 + 'cd_folder_'로 변경합니다

다음 명령을 실행하면 test1이라는 폴더가 생성됩니다. test1 마운트 폴더의 192.0.2.130 IP 주소에 vol1 볼륨을 마운트하고 새 test1 디렉토리로 변경합니다.

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 새 파일을 만들고 파일이 있는지 확인한 후 다음 파일에 텍스트를 씁니다.
   a. 테스트 파일을 만듭니다. + "touch_filename_"
   b. 파일이 있는지 확인합니다.: + "ls -l_filename_"
   c. cat>_filename_'을 입력합니다

      텍스트를 입력하고 Ctrl+D를 눌러 테스트 파일에 텍스트를 씁니다.

   d. 테스트 파일의 내용을 표시합니다. "cat_filename_"
   e. 테스트 파일: + "rm_filename_"을 제거합니다
   f. 상위 디렉토리로 돌아가기: + "cd…

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. 루트로 마운트된 볼륨에 대해 원하는 UNIX 소유권 및 권한을 설정합니다.
7. 내보내기 규칙에서 식별된 UNIX 클라이언트 시스템에서 이제 새 볼륨에 액세스할 수 있는 권한이 있는 사용자 중 하나로 로그인하고 3-5단계의 절차를 반복하여 볼륨을 마운트하고 파일을 생성할 수 있는지 확인합니다.