CLI를 사용하여 NFS를 구성합니다

ONTAP 9

NetApp
October 17, 2025

목차

CLI를 사용하여 NFS를 구성합니다 . . . 1
ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오 . . . 1
ONTAP에서 이 작업을 수행하는 다른 방법 . . . 1
ONTAP NFS 구성 워크플로에 대해 알아보세요 . . . 1
준비 . . . 2
ONTAP NFS의 물리적 스토리지 요구사항을 평가합니다 . . . 3
ONTAP NFS 네트워크 구성 요구 사항 평가 . . . 3
ONTAP NFS 스토리지 용량 프로비저닝에 대해 알아보십시오 . . . 5
ONTAP NFS 구성 워크시트 . . . 5
SVM에 대한 NFS 액세스를 구성합니다 . . . 14
NFS 데이터 액세스를 위한 ONTAP SVM 생성 . . . 14
ONTAP SVM에서 NFS 프로토콜 활성화 확인 . . . 16
ONTAP SVM에서 NFS 클라이언트 액세스 열기 . . . 17
ONTAP NFS 서버 생성 . . . 18
ONTAP NFS LIF를 생성합니다 . . . 20
ONTAP NFS SVM 호스트 이름 확인을 위해 DNS 활성화 . . . 24
이름 서비스 구성 . . . 25
강력한 보안을 위해 NFS와 Kerberos 사용 . . . 42
NFS 지원 SVM에 스토리지 용량 추가 . . . 48
ONTAP NFS 지원 SVM에 스토리지 용량을 추가하는 방법에 대해 알아보세요. . . . 48
ONTAP NFS 내보내기 정책 만들기 . . . 49
ONTAP NFS 내보내기 정책에 규칙 추가 . . . 49
볼륨 또는 qtree 스토리지 컨테이너를 생성합니다 . . . 54
내보내기 정책을 사용하여 NFS 액세스를 보호합니다 . . . 57
클러스터에서 ONTAP NFS 클라이언트 액세스를 확인하세요. . . . 59
클라이언트 시스템에서 ONTAP NFS 액세스 테스트 . . . 60
추가 ONTAP NFS 정보를 찾을 수 있는 곳 . . . 61
NFS 구성 . . . 62
네트워킹 구성 . . . 62
SAN 프로토콜 구성 . . . 62
루트 볼륨 보호 . . . 62
ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다릅니까 . . . 63
ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다릅니까 . . . 63
7-Mode 및 ONTAP NFS 내보내기 비교에 대해 알아보세요 . . . 63
ONTAP NFS 내보내기 정책 예제에 대해 알아보세요 . . . 64

CLI를 사용하여 NFS를 구성합니다

ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오

ONTAP 9 CLI 명령을 사용하여 새 SVM(스토리지 가상 머신) 또는 기존 SVM(스토리지 가상 머신)에서 새 볼륨 또는 qtree에 포함된 파일에 대한 NFS 클라이언트 액세스를 구성할 수 있습니다.

다음과 같은 방법으로 볼륨 또는 qtree에 대한 액세스를 구성하려면 다음 절차를 사용하십시오.

- 현재 ONTAP에서 지원하는 모든 버전의 NFS, NFSv3, NFSv4, NFSv4.1, NFSv4.2 또는 pNFS를 사용하는 NFSv4.1을 사용하려고 합니다.
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

  System Manager를 사용하여 NAS 멀티 프로토콜 액세스를 구성하려면 를 참조하십시오"NFS와 SMB를 모두 사용하여 Windows 및 Linux 모두에 대해 NAS 스토리지를 프로비저닝합니다".

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.

  명령 구문에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

- 새 볼륨의 보안을 위해 UNIX 파일 권한이 사용됩니다.
- SVM 관리자 권한이 아닌 클러스터 관리자 권한이 있습니다.

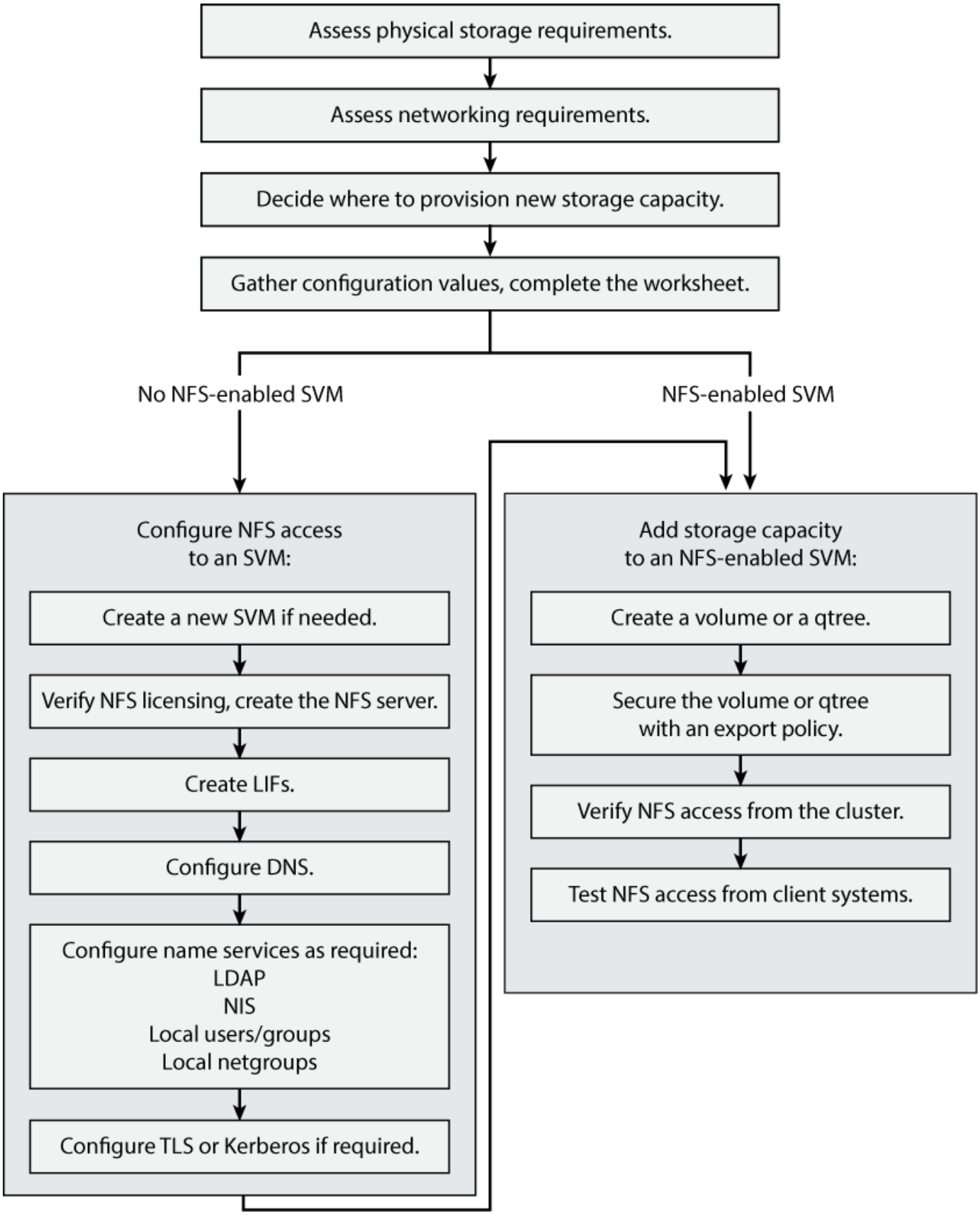
다양한 ONTAP NFS 프로토콜 기능에 대한 자세한 내용은 를 참조하십시오"NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요".

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면…	자세한 내용은…
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"NFS를 사용하여 Linux 서버용 NAS 스토리지 용량 할당"
System Manager Classic(ONTAP 9.7 이하에서 사용 가능	"NFS 구성 개요"

ONTAP NFS 구성 워크플로에 대해 알아보세요

NFS를 구성하려면 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음, 목표에 맞는 워크플로우를 선택해야 합니다. 새로운 SVM 또는 기존 SVM에 대한 NFS 액세스를 구성하거나, NFS 액세스를 위해 이미 완벽하게 구성된 기존 SVM에 볼륨 또는 qtree를 추가하십시오.


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access
to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity
to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree
with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

준비

ONTAP NFS의 물리적 스토리지 요구사항을 평가합니다

클라이언트용 NFS 스토리지를 프로비저닝하기 전에 새 볼륨에 대한 기존 애그리게이트에 충분한 공간이 있는지 확인해야 합니다. 없는 경우 디스크를 기존 Aggregate에 추가하거나 원하는 유형의 새 Aggregate를 생성할 수 있습니다.

단계

1. 기존 애그리게이트에서 사용 가능한 공간 표시:

   '스토리지 집계 쇼'

   공간이 충분한 집계가 있는 경우 워크시트에 이름을 기록합니다.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 충분한 공간이 있는 애그리게이트가 없는 경우 'Storage aggregate add-disks' 명령을 사용하여 기존 애그리게이트에 디스크를 추가하거나 'Storage aggregate create' 명령을 사용하여 새로운 애그리게이트를 생성합니다.

관련 정보

- "로컬 계층에 디스크 추가(애그리게이트)"
- "스토리지 집계 추가 디스크"
- "저장소 집계 생성"

ONTAP NFS 네트워크 구성 요구 사항 평가

NFS 스토리지를 클라이언트에 제공하기 전에 NFS 프로비저닝 요구 사항을 충족하도록 네트워킹이 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

다음과 같은 클러스터 네트워킹 객체를 구성해야 합니다.

- 물리적 및 논리적 포트
- 브로드캐스트 도메인
- 서브넷(필요한 경우)
- IPspace(기본 IPspace 외에 필요 시)
- 페일오버 그룹(필요에 따라 각 브로드캐스트 도메인의 기본 페일오버 그룹 추가)
- 외부 방화벽

단계

1. 사용 가능한 물리적 포트 및 가상 포트를 표시합니다.

   네트워크 포트 쇼

   - 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.
   - 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.
   - 에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 서브넷 이름을 사용하여 LIF에 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하는지, 사용 가능한 주소가 충분한지 확인합니다.

   네트워크 서브넷 쇼

   에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

   서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 서브넷은 network subnet create 명령을 사용하여 생성된다.

   에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 사용 가능한 IPspace 표시:

   네트워크 IPspace 쇼

   기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

   에 대한 자세한 내용은 `network ipspace show` "ONTAP 명령 참조입니다"을 참조하십시오.

4. IPv6 주소를 사용하려면 클러스터에서 IPv6이 활성화되어 있는지 확인합니다.

   네트워크 옵션 IPv6 쇼

   필요한 경우 'network options ipv6 modify' 명령을 사용하여 IPv6을 사용하도록 설정할 수 있습니다.

   및 `network options ipv6 modify` 에 대한 자세한 `network options ipv6 show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP NFS 스토리지 용량 프로비저닝에 대해 알아보십시오

새 NFS 볼륨 또는 qtree를 생성하기 전에 새로운 SVM이나 기존 SVM에 배치할지 여부와 SVM에 필요한 구성의 크기를 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

선택

- 새 SVM에서 볼륨 또는 qtree를 프로비저닝하거나 NFS가 활성화되어 있지만 구성되지 않은 기존 SVM에서 프로비저닝하려면 "SVM에 NFS 액세스 구성" 및 "NFS 스토리지를 NFS 지원 SVM에 추가" 단계를 완료하십시오.

  SVM에 대한 NFS 액세스를 구성합니다

  NFS 지원 SVM에 NFS 스토리지를 추가합니다

  다음 중 하나에 해당하는 경우 새 SVM을 생성할 수 있습니다.

  - 클러스터에서 NFS를 처음으로 사용하도록 설정하고 있습니다.
  - NFS 지원을 사용하지 않으려는 클러스터에 기존 SVM이 있습니다.
  - 하나의 클러스터에 NFS 지원 SVM이 하나 이상 있으며 다른 NFS 서버를 격리된 네임스페이스(멀티 테넌시 시나리오)로 사용하려는 경우를 가정해 보겠습니다. NFS가 활성화되었지만 구성되지 않은 기존 SVM에서 스토리지를 프로비저닝하려면 이 옵션을 선택해야 합니다. 이는 SAN 액세스를 위해 SVM을 생성했거나, SVM 생성 시 프로토콜을 사용하지 않은 경우에 발생할 수 있습니다.

  SVM에서 NFS를 사용하도록 설정한 후 볼륨 또는 qtree를 프로비저닝합니다.

- NFS 액세스를 위해 완전히 구성된 기존 SVM에서 볼륨 또는 qtree를 프로비저닝하려면 "NFS 스토리지를 NFS 지원 SVM에 추가"의 단계를 완료하십시오.

  NFS 지원 SVM에 NFS 스토리지 추가

ONTAP NFS 구성 워크시트

NFS 구성 워크시트를 사용하면 클라이언트에 대한 NFS 액세스를 설정하는 데 필요한 정보를 수집할 수 있습니다.

스토리지 용량 할당 위치에 대한 결정에 따라 워크시트의 섹션 중 하나 또는 두 섹션을 모두 완료해야 합니다.

SVM에 대한 NFS 액세스를 구성하는 경우 두 섹션을 모두 완료해야 합니다.

- SVM에 대한 NFS 액세스 구성
- NFS 지원 SVM에 스토리지 용량 추가

NFS 지원 SVM에 스토리지 용량을 추가하는 경우 다음 작업만 완료해야 합니다.

- NFS 지원 SVM에 스토리지 용량 추가

SVM에 대한 NFS 액세스를 구성합니다

- SVM 생성을 위한 매개 변수 *

새 SVM을 생성하는 경우 이러한 값을 'vserver create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	FQDN(정규화된 도메인 이름)이거나 클러스터 전체에 고유한 SVM 이름을 적용하는 다른 규칙을 따르는 새 SVM에 대해 제공하는 이름입니다.	
'-집계'	새 NFS 스토리지 용량을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-rootvolume'	SVM 루트 볼륨에 제공하는 고유 이름입니다.	
'-rootvolume-security-style'	SVM에 UNIX 보안 스타일을 사용합니다.	유닉스
'-언어'	이 워크플로의 기본 언어 설정을 사용합니다.	1. UTF-8
'IPSpace'	IPspace는 SVM(스토리지 가상 머신)이 상주하는 고유 IP 주소 공간입니다.	

- NFS 서버 생성을 위한 매개 변수 *

새 NFS 서버를 생성하고 지원되는 NFS 버전을 지정할 때 이러한 값을 'vserver NFS create' 명령으로 제공합니다.

NFSv4 이상을 설정하는 경우 보안을 강화하기 위해 LDAP를 사용해야 합니다.

필드에 입력합니다	설명	귀사의 가치
v3 -v4.0 -v4.1 -v4.1 -v4.1 -pNFS	필요에 따라 NFS 버전을 사용하도록 설정합니다. v4.2는 v4.1이 활성화된 경우 ONTAP 9.8 이상에서도 지원됩니다.	
'-v4-id-domain'	ID 매핑 도메인 이름입니다.	
'-v4-numeric-ids'	숫자 소유자 ID 지원(사용 또는 사용 안 함)	

- LIF 생성을 위한 매개 변수 *

LIF를 생성할 때 이러한 값을 명령과 함께 `network interface create` 제공합니다. 에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

Kerberos를 사용하는 경우 여러 LIF에서 Kerberos를 사용하도록 설정해야 합니다.

필드에 입력합니다	설명	귀사의 가치
'-lif'	새 LIF에 대해 제공한 이름입니다.	
'-역할'	이 워크플로우에서 데이터 LIF 역할을 사용합니다.	다타
'-데이터-프로토콜'	이 워크플로우에서는 NFS 프로토콜만 사용합니다.	'NFS'입니다
홈 노드	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행할 때 LIF가 반환되는 노드입니다. 에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.	
``홈 포트''	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 포트 또는 인터페이스 그룹입니다.	
주소	새 LIF가 데이터 액세스에 사용할 클러스터의 IPv4 또는 IPv6 주소입니다.	
넷마스크입니다	LIF의 네트워크 마스크와 게이트웨이입니다.	
'-서브넷'	IP 주소 풀입니다. 주소와 넷마스크를 자동으로 할당하기 위해 -address와 -netmask 대신 사용됩니다.	
방화벽 정책	이 워크플로우에서 기본 데이터 방화벽 정책을 사용합니다.	다타

- DNS 호스트 이름 확인을 위한 매개 변수 *

DNS를 구성할 때 이러한 값을 'vserver services name-service dns create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치
``도메인’	최대 5개의 DNS 도메인 이름	
이름-서버	각 DNS 이름 서버에 대해 최대 3개의 IP 주소를 지정할 수 있습니다.	

네임 서비스 정보

- 로컬 사용자 생성을 위한 매개 변수 *

'vserver services name-service unix-user create' 명령을 사용하여 로컬 사용자를 생성하는 경우 이러한 값을 제공합니다. UNIX 사용자가 포함된 파일을 URI(Uniform Resource Identifier)에서 로드하여 로컬 사용자를 구성하는 경우에는 이러한 값을 수동으로 지정할 필요가 없습니다.

	사용자 이름 '(-user)'입니다	사용자 ID '(-id)'입니다	그룹 ID '(-primary-gid)'입니다	전체 이름(-full-name)
예	합니다	123을 선택합니다	100	존 밀러
1				
2				
3				
…				
해당 없음				

- 로컬 그룹 생성을 위한 매개 변수 *

'vserver services name-service unix-group create' 명령을 사용하여 로컬 그룹을 생성하는 경우 이러한 값을 제공합니다. URI에서 UNIX 그룹이 포함된 파일을 로드하여 로컬 그룹을 구성하는 경우에는 이러한 값을 수동으로 지정할 필요가 없습니다.

	그룹 이름('-name')	Group ID('-id')
예	엔지니어링	100
1		
2		
3		
…		

해당 없음		

- NIS용 매개 변수 *

이러한 값은 'vserver services name-service NIS-domain create' 명령을 사용하여 입력합니다.

그만큼 `-nis-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-nis-servers` NIS 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

필드에 입력합니다	설명	귀사의 가치
``도메인’	SVM이 이름 조회에 사용할 NIS 도메인입니다.	
'-활성'	활성 NIS 도메인 서버입니다.	참 거짓입니다
'-NIS-서버'	도메인 구성에 사용되는 NIS 서버의 IP 주소와 호스트 이름을 쉼표로 구분한 목록입니다.	

- LDAP용 매개 변수 *

이러한 값은 'vserver services name-service ldap client create' 명령을 사용하여 입력합니다.

자체 서명된 루트 CA 인증서 '.pem' 파일도 필요합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	LDAP 클라이언트 구성을 생성할 SVM의 이름입니다.	
'-client-config’입니다	새 LDAP 클라이언트 구성에 할당한 이름입니다.	
'-LDAP-서버'	LDAP 서버의 IP 주소 및 호스트 이름을 쉼표로 구분하여 나열합니다.	
'-query-timeout’입니다	이 워크플로에 기본 3초를 사용합니다.	3
'-min-bind-level'	최소 바인딩 인증 수준입니다. 기본값은 'anonymous’입니다. 서명 및 봉인을 구성한 경우 'ASL’으로 설정해야 합니다.	

필드에 입력합니다	설명	귀사의 가치
'-preferred-ad-servers'	쉼표로 구분된 목록에서 IP 주소별로 하나 이상의 기본 Active Directory 서버가 있습니다.	
'-ad-domain'입니다	Active Directory 도메인입니다.	
'-스키마'	사용할 스키마 템플릿입니다. 기본 스키마나 사용자 지정 스키마를 사용할 수 있습니다.	
``포트''	이 워크플로우에는 기본 LDAP 서버 포트 '389'를 사용합니다.	389
'-bind-dn'	Bind 사용자 고유 이름입니다.	
'-base-dn'	기본 고유 이름입니다. 기본값은 ""(root)입니다.	
``기본범위''	이 워크플로에 기본 기본 검색 범위 'Subnet'을 사용합니다.	'우방'
'-세션-보안'	LDAP 서명 또는 서명 및 봉인을 활성화합니다. 기본값은 '없음'입니다.	
'-use-start-tls'	TLS를 통해 LDAP를 활성화합니다. 기본값은 false 입니다.	

- Kerberos 인증 매개변수 *

이러한 값은 'vserver NFS Kerberos realm create' 명령을 사용하여 입력합니다. 일부 값은 KDC(Key Distribution Center) 서버로 Microsoft Active Directory를 사용할지, MIT 또는 기타 UNIX KDC 서버를 사용하는지에 따라 달라집니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	KDC와 통신할 SVM.	
``영역'	Kerberos 영역.	
시계 편중	클라이언트와 서버 간에 허용되는 클럭 편중.	
'-KDC-IP'	KDC IP 주소입니다.	

``KDC-포트’	KDC 포트 번호입니다.	
'-adserver-name’입니다	Microsoft KDC 전용: AD 서버 이름입니다.	
'-adserver-ip’입니다	Microsoft KDC 전용: AD 서버 IP 주소입니다.	
'-AdminServer-IP’입니다	UNIX KDC 전용: 관리 서버 IP 주소.	
'-AdminServer-port’입니다	UNIX KDC만 해당: 관리 서버 포트 번호입니다.	
'-passwordserver-IP’입니다	UNIX KDC 전용: 암호 서버 IP 주소입니다.	
'-passwordserver-port’입니다	UNIX KDC 전용: 암호 서버 포트.	
``KDC-벤더’	KDC 공급업체.	{'Microsoft'
'기타'}	``논평’	원하는 코멘트.

이러한 값은 'vserver NFS Kerberos interface enable' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	Kerberos 구성을 생성할 SVM의 이름입니다.	
'-lif'	Kerberos를 사용하도록 설정할 데이터 LIF입니다. 여러 LIF에서 Kerberos를 사용하도록 설정할 수 있습니다.	
'-SPN'	서비스 원칙 이름(SPN)	
``허용된-원력-유형’’	클라이언트 기능에 따라 Kerberos over NFS에 대해 허용되는 암호화 유형인 AES-256을 사용하는 것이 좋습니다.	
'-admin-username’입니다	KDC에서 직접 SPN 암호 키를 검색하는 KDC 관리자 자격 증명입니다. 암호가 필요합니다	

'-keytab-Uri’입니다	KDC 관리자 자격 증명이 없는 경우 SPN 키가 포함된 KDC의 keytab 파일입니다.	
'-ou'	Microsoft KDC의 영역을 사용하여 Kerberos를 설정할 때 Microsoft Active Directory 서버 계정이 생성되는 OU(조직 구성 단위)입니다.	

NFS 지원 **SVM**에 스토리지 용량 추가

- 내보내기 정책 및 규칙 생성을 위한 매개 변수 *

이러한 값은 'vserver export-policy create' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	새 볼륨을 호스팅할 SVM의 이름입니다.	
정책 이름	새 엑스포트 정책에 대해 제공한 이름입니다.	

각 규칙에 대해 'vserver export-policy rule create' 명령을 사용하여 이러한 값을 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-clientmatch'	클라이언트 일치 사양.	
룰레인덱스	규칙 목록에서 내보내기 규칙의 위치입니다.	
'-프로토콜'	이 워크플로우에서 NFS를 사용합니다.	'NFS’입니다
'-rorule'	읽기 전용 액세스에 대한 인증 방법입니다.	
'-rwrule'	읽기-쓰기 액세스를 위한 인증 방법입니다.	
'-슈퍼유저'	고급 사용자 액세스를 위한 인증 방법입니다.	
'-anon'	익명 사용자가 매핑되는 사용자 ID입니다.	

각 엑스포트 정책에 대해 하나 이상의 규칙을 생성해야 합니다.

'-ruleindex'	'* - clientmatch * '	' * -rorule * '	'*-rwrule * '	'*-슈퍼유저 * '	'*-anon * '
예	0.0.0.0/0, @rootaccess_netgroup	모두	krb5	시스템	65534
1					
2					
3					
…					
해당 없음					

- 볼륨 생성을 위한 매개 변수 *

Qtree 대신 볼륨을 생성하는 경우 이 값에 'volume create' 명령을 입력합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	새 볼륨을 호스팅할 새 SVM 또는 기존 SVM의 이름입니다.	
'- 볼륨'	새 볼륨에 제공하는 고유한 설명 이름입니다.	
'-집계'	새 NFS 볼륨을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-size'	새 볼륨의 크기에 대해 제공하는 정수입니다.	
'-user'	볼륨 루트의 소유자로 설정된 사용자의 이름 또는 ID입니다.	
``그룹''	볼륨 루트의 소유자로 설정된 그룹의 이름 또는 ID입니다.	
``보안스타일''	이 워크플로우에는 UNIX 보안 스타일을 사용합니다.	유닉스

``교차점-경로''	새 볼륨을 마운트할 루트(/) 아래의 위치입니다.	
수출정책	기존 엑스포트 정책을 사용하려는 경우 볼륨을 생성할 때 해당 이름을 입력할 수 있습니다.	

- qtree 생성을 위한 매개 변수 *

볼륨 대신 qtree를 생성하는 경우 이 값에 'volume qtree create' 명령을 입력합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	qtree가 포함된 볼륨이 있는 SVM의 이름입니다.	
'- 볼륨'	새 qtree를 포함할 볼륨의 이름입니다.	
'-qtree'	새 qtree를 64자 이하로 설명하는 고유한 이름입니다.	
'-qtree-path'	볼륨과 qtree를 별도의 인수로 지정하는 대신 '/vol/*volume_name/qtree_name*\>' 형식의 qtree 경로 인수를 지정할 수 있습니다.	
'-unix-permissions'	선택 사항: qtree에 대한 UNIX 사용 권한	
수출정책	기존 엑스포트 정책을 사용하려는 경우 qtree를 생성할 때 이름을 입력할 수 있습니다.	

관련 정보

- "ONTAP 명령 참조입니다"

SVM에 대한 NFS 액세스를 구성합니다

NFS 데이터 액세스를 위한 ONTAP SVM 생성

NFS 클라이언트에 데이터 액세스를 제공하기 위해 클러스터에 SVM이 하나 이상 없으면 하나 이상의 SVM을 생성해야 합니다.

시작하기 전에

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할

경우에도 경고를 구성할 수 있습니다. 자세한 내용은 을 SVM 용량 관리참조하십시오.

단계

1. SVM 생성:

   'vserver create-vserver_vserver_name_-rootvolume_root_volume_name_-aggregate_aggregate_name_-rootvolume-security-style UNIX-language C. UTF-8-IPSpace_IPSpace_name_'

   - '-rootvolume-security-style' 옵션에 UNIX 설정을 사용합니다.
   - 기본 C. UTF-8 '-language' 옵션을 사용합니다.
   - IPSpace 설정은 선택 사항입니다.

2. 새로 생성한 SVM의 구성 및 상태 확인:

   'vserver show -vserver_vserver_name_'

   허용되는 프로토콜 필드는 NFS를 포함해야 합니다. 나중에 이 목록을 편집할 수 있습니다.

   'Vserver 작동 상태' 필드에는 '실행 중' 상태가 표시되어야 합니다. 초기화 중 상태가 표시되는 경우 루트 볼륨 생성 등 일부 중간 작업이 실패한 것으로, SVM을 삭제하고 다시 생성해야 합니다.

예

다음 명령은 IPspace에서 데이터 액세스를 위한 SVM을 생성합니다. spaceba:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

다음 명령을 실행하면 루트 볼륨 1GB 단위로 SVM이 생성되고 자동으로 시작되어 '실행 중' 상태에 있음을 알 수 있습니다. 루트 볼륨에는 규칙을 포함하지 않는 기본 엑스포트 정책이 있으므로 생성 시 루트 볼륨을 내보내지 않습니다.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 적응형 정책 그룹 템플릿을 설정합니다참조하십시오.

ONTAP SVM에서 NFS 프로토콜 활성화 확인

SVM에서 NFS를 구성 및 사용하려면 먼저 프로토콜이 활성화되어 있는지 확인해야 합니다.

이 작업에 대해

이는 일반적으로 SVM 설정 중에 수행되지만 설정 중에 프로토콜을 활성화하지 않은 경우 나중에 'vserver add-protocols' 명령을 사용하여 활성화할 수 있습니다.

프로토콜을 생성한 후에는 LIF에서 프로토콜을 추가하거나 제거할 수 없습니다.

"vserver remove-protocols" 명령을 사용하여 SVM에서 프로토콜을 비활성화할 수도 있습니다.

단계

1. 현재 SVM에 대해 활성화 및 비활성화된 프로토콜을 확인합니다.

'vserver show -vserver_vserver_name_-protocols'

"vserver show-protocols" 명령을 사용하여 클러스터의 모든 SVM에서 현재 활성화된 프로토콜을 볼 수도 있습니다.

2. 필요한 경우 프로토콜을 활성화 또는 비활성화합니다.
   - NFS 프로토콜을 활성화하려면: + 'vserver add-protocols-vserver_vserver_name_-protocols nfs'
   - 프로토콜을 작동 불가능하게 하려면: + "vserver remove-protocols-vserver_name_-protocols_protocol_name_[,*protocol_name*,…]
3. 활성화된 프로토콜과 비활성화된 프로토콜이 올바르게 업데이트되었는지 확인합니다.

   'vserver show -vserver_vserver_name_-protocols'

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 현재 설정 및 해제된 프로토콜(허용 및 허용 안 함)이 표시됩니다.

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

다음 명령을 사용하면 이름이 VS1 인 SVM에서 활성화된 프로토콜 목록에 NFS를 추가하여 NFS를 통해 액세스할 수 있습니다.

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

ONTAP SVM에서 NFS 클라이언트 액세스 열기

SVM 루트 볼륨의 기본 엑스포트 정책에는 NFS를 통해 모든 클라이언트가 액세스할 수 있도록 하는 규칙이 포함되어야 합니다. 이 규칙이 없으면 모든 NFS 클라이언트가 SVM 및 해당 볼륨에 대한 액세스가 거부됩니다.

이 작업에 대해

새 SVM이 생성되면 SVM의 루트 볼륨에 대한 기본 엑스포트 정책(기본값)이 자동으로 생성됩니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 엑스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다.

기본 엑스포트 정책에서 모든 NFS 클라이언트에 대한 액세스가 허용되는지 확인하고, 나중에 개별 볼륨 또는 qtree에 대한 사용자 지정 엑스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. 기존 SVM을 사용하는 경우 기본 루트 볼륨 엑스포트 정책을 확인하십시오.

   'vserver export-policy rule show'를 선택합니다

   명령 출력은 다음과 같아야 합니다.

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

이러한 규칙이 열려 있는 액세스를 허용하는 경우 이 작업은 완료된 것입니다. 그렇지 않은 경우 다음 단계를 진행하십시오.

2. SVM 루트 볼륨에 대한 엑스포트 규칙 생성:

   'vserver export-policy rule create-vserver_vserver_name_-policyname default-ruleindex 1-protocol nfs-clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any'

   SVM이 Kerberos로 보호되는 볼륨만 포함할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5' 또는 'krb5i'로 설정할 수 있습니다. 예를 들면 다음과 같습니다.

   '-rorule krb5i-rwrule krb5i-superuser krb5i'

3. 'vserver export-policy rule show' 명령을 사용하여 규칙 생성을 확인합니다.

결과

이제 모든 NFS 클라이언트가 SVM에서 생성된 모든 볼륨 또는 qtree에 액세스할 수 있습니다.

ONTAP NFS 서버 생성

클러스터에서 NFS 라이센스가 등록되었는지 확인한 후 "vserver NFS create" 명령을 사용하여 SVM에 NFS 서버를 생성하고 해당 명령이 지원하는 NFS 버전을 지정할 수 있습니다.

이 작업에 대해

SVM은 하나 이상의 NFS 버전을 지원하도록 구성할 수 있습니다. NFSv4 이상을 지원하는 경우:

- NFSv4 사용자 ID 매핑 도메인 이름은 NFSv4 서버 및 타겟 클라이언트에서 동일해야 합니다.

  NFSv4 서버와 클라이언트가 동일한 이름을 사용하는 한 LDAP 또는 NIS 도메인 이름과 같을 필요는 없습니다.

- 타겟 클라이언트는 NFSv4 숫자 ID 설정을 지원해야 합니다.
- 보안을 위해 NFSv4 구축에서는 이름 서비스에 LDAP를 사용해야 합니다.

시작하기 전에

SVM은 NFS 프로토콜을 허용하도록 구성해야 합니다.

단계

1. NFS 라이센스가 클러스터에서 라이센스되었는지 확인합니다.

   'system license show-package nfs'

   그렇지 않은 경우 영업 담당자에게 문의하십시오.

2. NFS 서버 생성:

   'vserver NFS create -vserver_vserver_name_-v3{enabled | disabled} -v4.0{enabled | disabled} -v4-id -domain_NFSv4_id_domain_-v4-numeric-ids{enabled | disabled} -v4.1{enabled | disabled | pNFS{enabled | disabled}'를 선택합니다

   NFS 버전의 조합을 사용하도록 선택할 수 있습니다. pNFS를 지원하려면 '-v4.1'과 '-v4.1-pNFS' 옵션을 모두 사용해야 합니다.

   v4 이상을 사용하는 경우 다음 옵션도 올바르게 설정되어 있어야 합니다.

   - '-v4-id-domain'

     이 선택적 매개 변수는 NFSv4 프로토콜에서 정의된 사용자 및 그룹 이름의 문자열 형식 도메인 부분을 지정합니다. 기본적으로 ONTAP는 NIS 도메인이 설정되어 있는 경우 NIS 도메인을 사용하고, 설정되어 있지 않으면 DNS 도메인이 사용됩니다. 대상 클라이언트가 사용하는 도메인 이름과 일치하는 값을 입력해야 합니다.

   - '-v4-numeric-ids'

     이 선택적 매개 변수는 NFSv4 소유자 속성에서 숫자 문자열 식별자를 지원하도록 설정되었는지 여부를 지정합니다. 기본 설정은 활성화되지만 타겟 클라이언트가 이 설정을 지원하는지 확인해야 합니다.

   나중에 'vserver nfs modify' 명령을 사용하여 추가 NFS 기능을 활성화할 수 있습니다.

3. NFS가 실행 중인지 확인합니다.

   'vserver NFS status-vserver_vserver_name_'

4. NFS가 원하는 대로 구성되었는지 확인합니다.

   'vserver nfs show -vserver_vserver_name_'

예

다음 명령을 실행하면 NFSv3 및 NFSv4.0이 설정된 VS1 이라는 SVM에 NFS 서버가 생성됩니다.

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

다음 명령을 실행하면 이름이 VS1 인 새 NFS 서버의 상태와 구성 값이 검증됩니다.

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                                Vserver: vs1
                    General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                           UDP Protocol: enabled
                           TCP Protocol: enabled
                  Default Windows User: -
                   NFSv4.0 ACL Support: disabled
      NFSv4.0 Read Delegation Support: disabled
     NFSv4.0 Write Delegation Support: disabled
              NFSv4 ID Mapping Domain: my_domain.com
...
```

ONTAP NFS LIF를 생성합니다

LIF는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트로 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

  서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 네트워크 서브넷 만들기 명령을 사용하여 만듭니다.

  에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

이 작업에 대해

- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- Kerberos 인증을 사용하는 경우 여러 LIF에서 Kerberos를 사용하도록 설정합니다.
- 클러스터에 LIF가 많은 경우 'network interface capacity show' 명령을 사용하여 클러스터에서 지원되는 LIF 용량과 각 노드에서 지원되는 LIF 용량을 확인할 수 있습니다 (고급 권한 수준에서).

및 `network interface capacity details show` 에 대한 자세한 `network interface capacity show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

ONTAP 9.4부터는 FC-NVMe가 지원됩니다. FC-NVMe LIF를 생성하는 경우 다음 사항을 알아야 합니다.

- NVMe 프로토콜은 LIF가 생성된 FC 어댑터에서 지원되어야 합니다.
- FC-NVMe는 데이터 LIF에서 유일한 데이터 프로토콜일 수 있습니다.
- SAN을 지원하는 모든 SVM(스토리지 가상 머신)에서 관리 트래픽을 처리하는 하나의 LIF를 구성해야 합니다.
- NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
- SVM당 하나의 NVMe LIF에서 데이터 트래픽을 처리할 수 있습니다

단계

1. LIF 생성:

   'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol nfs-home-node_node_name_-home-port_port_name_{-address_{-address_netmask_ip_address_|-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true|false}

   에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

옵션을 선택합니다	설명
• ONTAP 9.5 이하 *	'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol nfs-home-node_node_name_-home-port_port_name_{-address_{-address_netmask_ip_address_
-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true	false}
• ONTAP 9.6 이상 *	'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol nfs-home-node_node_name_-home-port_port_name_{-address_{-address_netmask_ip_address_
-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true	false}

- 서비스 정책(ONTAP 9.6에서 시작)을 사용하여 LIF를 생성할 때는 '-role' 매개 변수가 필요하지 않습니다.
- LIF를 생성할 때 '-data-protocol' 매개 변수를 지정해야 하며 나중에 데이터 LIF를 삭제 및 다시 생성하지 않고 수정할 수 없습니다.

  서비스 정책(ONTAP 9.6부터)을 사용하여 LIF를 생성할 때는 '-data-protocol' 매개 변수가 필요하지 않습니다.

- 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도 있습니다.

에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.

- '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
- IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
- 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.
- 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 `network route create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.
- '-firewall-policy' 옵션의 경우 LIF 역할과 동일한 기본 data를 사용합니다.

  필요에 따라 나중에 사용자 지정 방화벽 정책을 만들고 추가할 수 있습니다.

  ⓘ ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

- '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 false로 설정할 수 있습니다.

  a. 'network interface show' 명령을 사용하여 LIF가 성공적으로 생성되었는지 확인합니다.

  b. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면…	사용…
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

  c. Kerberos를 사용하는 경우 1단계부터 3단계까지 반복하여 추가 LIF를 생성합니다.

  Kerberos는 이러한 각 LIF에서 별도로 설정해야 합니다.

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 cluster-1의 모든 LIF가 표시됩니다. 데이터 LIF datalif1 및 datalif3은 IPv4 주소로 구성되고 datalif4는 IPv6 주소로 구성됩니다.

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

다음 명령을 실행하면 기본 데이터 파일 서비스 정책에 할당된 NAS 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스"

ONTAP NFS SVM 호스트 이름 확인을 위해 DNS 활성화

SVM에서 DNS를 사용하도록 설정하려면 'vserver services name-service dns' 명령을 사용하고, 호스트 이름 확인을 위해 DNS를 사용하도록 구성할 수 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. DNS 서버 이름을 하나만 입력하면 'vserver services name-service dns create' 명령이 경고를 보냅니다.

이 작업에 대해

에 대해 자세히 "SVM에서 동적 DNS 구성"알아보십시오.

단계

1. SVM에서 DNS 활성화:

   'vserver services name-service dns create-vserver_vserver_name_-domain_domain_name_-name-servers_ip_address_-state enabled'

   다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   를 클릭합니다 `vserver services name-service dns create` Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. 'vserver services name-service dns show' 명령을 사용하여 DNS 도메인 구성을 표시합니다.

   다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

```
vserver services name-service dns show
                                                 Name
Vserver           State     Domains              Servers
----------------- --------- -------------------- -------------
cluster1          enabled   example.com          192.0.2.201,
                                                 192.0.2.202
vs1.example.com   enabled   example.com          192.0.2.201,
                                                 192.0.2.202
```

다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

이름 서비스 구성

ONTAP NFS 이름 서비스에 대해 알아보세요

스토리지 시스템의 구성에 따라 ONTAP는 클라이언트에 대한 적절한 액세스를 제공하기 위해 호스트, 사용자, 그룹 또는 넷그룹 정보를 조회해야 합니다. 이 정보를 얻으려면 ONTAP가 로컬 또는 외부 이름 서비스에 액세스하도록 이름 서비스를 구성해야 합니다.

클라이언트 인증 중에 NIS 또는 LDAP와 같은 이름 서비스를 사용하여 이름 조회를 용이하게 해야 합니다. 특히 NFSv4 이상을 구축할 때 보안을 강화하기 위해 가능하면 LDAP를 사용하는 것이 좋습니다. 또한 외부 이름 서버를 사용할 수 없는 경우 로컬 사용자 및 그룹을 구성해야 합니다.

이름 서비스 정보는 모든 소스에서 동기화되어야 합니다.

ONTAP NFS 이름 서비스 스위치 테이블 구성

ONTAP가 로컬 또는 외부 이름 서비스에 문의하여 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑 정보를 검색할 수 있도록 이름 서비스 스위치 테이블을 올바르게 구성해야 합니다.

시작하기 전에

사용자 환경에 적용할 수 있는 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑에 사용할 이름 서비스를 결정해야 합니다.

넷그룹을 사용할 계획이라면 RFC 5952에 지정된 대로 넷그룹에 지정된 모든 IPv6 주소를 단축하고 압축해야 합니다.

이 작업에 대해

사용하지 않는 정보 소스는 포함하지 마십시오. 예를 들어 NIS가 사용자 환경에서 사용되지 않는 경우 '-Sources NIS' 옵션을 지정하지 마십시오.

단계

1. 이름 서비스 스위치 테이블에 필요한 항목을 추가합니다.

   'vserver services name-service ns-switch create-vserver_vserver_name_-database_database_name_-sources_source_names_'

2. 이름 서비스 스위치 테이블에 원하는 순서대로 필요한 항목이 포함되어 있는지 확인합니다.

   'vserver services name-service ns-switch show -vserver_vserver_name_'

   수정하려면 'vserver services name-service ns-switch modify' 또는 'vserver services name-service ns-switch delete' 명령을 사용해야 합니다.

예

다음 예에서는 SVM VS1 에서 로컬 넷그룹 파일을 사용할 수 있도록 이름 서비스 스위치 테이블에 새 항목을 생성하고 외부 NIS 서버에서 넷그룹 정보를 순서대로 찾습니다.

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

작업을 마친 후

- 데이터 액세스를 제공하려면 SVM에 지정한 이름 서비스를 구성해야 합니다.
- SVM에 대한 네임 서비스를 삭제할 경우 네임 서비스 스위치 테이블에서 해당 서비스를 제거해야 합니다.

  이름 서비스 스위치 테이블에서 이름 서비스를 삭제하지 않으면 스토리지 시스템에 대한 클라이언트 액세스가 예상대로 작동하지 않을 수 있습니다.

로컬 **UNIX** 사용자 및 그룹을 구성합니다

ONTAP NFS SVM에 대한 로컬 **UNIX** 사용자 및 그룹에 대해 알아보세요**.**

SVM에서 로컬 UNIX 사용자 및 그룹을 사용하여 인증 및 이름 매핑을 수행할 수 있습니다. UNIX 사용자 및 그룹을 수동으로 만들거나 UNIX 사용자 또는 그룹이 포함된 파일을 URI(Uniform

Resource Identifier)에서 로드할 수 있습니다.

클러스터에 결합된 로컬 UNIX 사용자 그룹 및 그룹 구성원의 기본 최대 제한은 32,768입니다. 클러스터 관리자가 이 제한을 수정할 수 있습니다.

ONTAP NFS SVM에서 로컬 UNIX 사용자 생성

'vserver services name-service unix-user create' 명령을 사용하여 로컬 UNIX 사용자를 생성할 수 있습니다. 로컬 UNIX 사용자는 이름 매핑 처리에 사용되는 UNIX 이름 서비스 옵션으로 SVM에서 생성하는 UNIX 사용자입니다.

단계

1. 로컬 UNIX 사용자 생성:

   'vserver services name-service unix-user create-vserver_vserver_name_-user_user_name_-id_integer_-primary-gid_integer_-full-name_full_name_'

   '-user_user_name_'은(는) 사용자 이름을 지정합니다. 사용자 이름의 길이는 64자 이하여야 합니다.

   '-id_integer_'는 사용자가 지정하는 사용자 ID를 지정합니다.

   기본 그룹 ID는 -primary-gid_integer_ 로 지정합니다. 그러면 사용자가 기본 그룹에 추가됩니다. 사용자를 생성한 후 원하는 추가 그룹에 사용자를 수동으로 추가할 수 있습니다.

예

다음 명령을 실행하면 이름이 johnm인 로컬 UNIX 사용자가 이름이 vs1 인 SVM에 생성됩니다. 사용자는 ID 123 및 기본 그룹 ID 100을 가지고 있습니다.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

ONTAP NFS SVM에 로컬 UNIX 사용자 목록 로드

SVM에서 개별 로컬 UNIX 사용자를 수동으로 생성하는 대신 로컬 UNIX 사용자 목록을 URI(Uniform Resource Identifier)에서 SVM으로 로드하여 작업을 단순화할 수 있습니다('vserver services name-service unix-user load-from-Uri').

단계

1. 로드할 로컬 UNIX 사용자 목록이 포함된 파일을 생성합니다.

   파일은 UNIX '/etc/passwd' 형식의 사용자 정보를 포함해야 합니다.

   '*user_name:password:user_ID:group_ID:full_name*'

   명령에서는 '*PASSWORD*' 필드 값과 '*FULL_NAME*' 필드 뒤에 있는 필드 값('*HOME_DIRECTORY*' 및 '*shell*')이 삭제됩니다.

지원되는 최대 파일 크기는 2.5MB입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

   목록에 중복 항목이 포함되어 있으면 목록을 로드하지 못하고 오류 메시지가 표시됩니다.

3. 파일을 서버에 복사합니다.

   스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

   URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 사용자 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

   'vserver services name-service unix-user load-from-Uri-vserver_vserver_name_-Uri{ftp|http|ftps|https}://*Uri* -overwrite{true|false}'

   '-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/passwd` 에서 이름이 VS1 인 SVM으로 로컬 UNIX 사용자 목록이 로드됩니다. SVM의 기존 사용자는 URI의 정보로 덮어써지지 않습니다.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

ONTAP NFS SVM에 로컬 **UNIX** 그룹 생성

"vserver services name-service unix-group create" 명령을 사용하여 SVM에 로컬인 UNIX 그룹을 생성할 수 있습니다. 로컬 UNIX 그룹은 로컬 UNIX 사용자와 함께 사용됩니다.

단계

1. 로컬 UNIX 그룹 생성:

   'vserver services name-service unix-group create-vserver_vserver_name_-name_group_name_-id_integer_'

   `-name_group_name_'은 그룹 이름을 지정합니다. 그룹 이름의 길이는 64자 이하여야 합니다.

   '-id_integer_'는 지정하는 그룹 ID를 지정합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 eng인 로컬 그룹이 생성됩니다. 그룹에 ID 101이 있습니다.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

ONTAP NFS SVM의 로컬 **UNIX** 그룹에 사용자 추가

'vserver services name-service unix-group adduser' 명령을 사용하여 SVM에 로컬인 보조 UNIX 그룹에 사용자를 추가할 수 있습니다.

단계

1. 로컬 UNIX 그룹에 사용자 추가:

'vserver services name-service unix-group adduser-vserver_vserver_name_-name_group_name_-username_user_name_'

'-name"*group_name*'은 사용자의 기본 그룹 외에도 사용자를 추가할 UNIX 그룹의 이름을 지정합니다.

예

다음 명령을 실행하면 이름이 max인 사용자가 이름이 eng인 로컬 UNIX 그룹에 이름이 vs1 인 SVM에 추가됩니다.

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

ONTAP NFS SVM의 **URI**에서 로컬 **UNIX** 그룹 로드

개별 로컬 UNIX 그룹을 수동으로 생성하는 대신 'vserver services name-service unix-group load-from-Uri' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 로컬 UNIX 그룹 목록을 로드할 수 있습니다.

단계

1. 로드할 로컬 UNIX 그룹 목록이 포함된 파일을 생성합니다.

   파일은 UNIX '/etc/group' 형식의 그룹 정보를 포함해야 합니다.

   '*group_name:password:group_ID:comma_separated_list_of_users*'

   이 명령어는 '*PASSWORD*' 필드의 값을 삭제한다.

   지원되는 최대 파일 크기는 1MB입니다.

   그룹 파일에서 각 줄의 최대 길이는 32,768자입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

   목록에 중복 항목이 없어야 합니다. 그렇지 않으면 목록을 로드하지 못합니다. SVM에 이미 있는 항목이 있으면 "-overwrite" 매개 변수를 "true"로 설정하여 모든 기존 항목을 새 파일로 덮어쓰거나 새 파일에 기존 항목을 복제하는 항목이 없는지 확인해야 합니다.

3. 파일을 서버에 복사합니다.

   스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

   URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 그룹 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

   'vserver services name-service unix-group load-from-Uri-vserver_vserver_name_-Uri{ftp|http|FTPS|https}://*Uri*-overwrite{true|false}'

   '-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다. 이 매개 변수를 "true"로 지정하면 ONTAP는 지정된 SVM의 기존 로컬 UNIX 그룹 데이터베이스 전체를 로드하는 파일의 항목으로 바꿉니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/group` 에서 VS1 이라는 SVM으로 로컬 UNIX 그룹 목록이 로드됩니다. SVM의 기존 그룹은 URI의 정보로 덮어써지지 않습니다.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

넷그룹으로 작업합니다

ONTAP NFS SVM의 넷그룹에 대해 알아보세요

사용자 인증 및 내보내기 정책 규칙의 클라이언트와 일치시키기 위해 넷그룹을 사용할 수 있습니다. 외부 이름 서버(LDAP 또는 NIS)에서 넷그룹에 대한 액세스를 제공하거나, 'vserver services name-service netgroup load' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다.

시작하기 전에

넷그룹을 사용하기 전에 다음 조건이 충족되는지 확인해야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹의 모든 호스트는 순방향 및 역방향 DNS 조회를 일관되게 제공하기 위해 정방향(A) 및 역방향(PTR) DNS 레코드를 모두 포함해야 합니다.

  또한 클라이언트의 IP 주소에 PTR 레코드가 여러 개 있는 경우 이러한 모든 호스트 이름은 넷그룹의 구성원이어야 하며 해당 레코드가 있어야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹에 있는 모든 호스트의 이름은 철자가 올바르고 올바른 대소문자를 사용해야 합니다. 넷그룹에서 사용되는 호스트 이름의 대/소문자 불일치로 인해 내보내기 검사 실패와 같은 예기치 않은 동작이 발생할 수 있습니다.
- 넷그룹에 지정된 모든 IPv6 주소는 RFC 5952에 지정된 대로 단축되고 압축되어야 합니다.

  예를 들어 2011:hu9:0:0:0:0:3:1은 2011:hu9:3:1로 단축되어야 합니다.

이 작업에 대해

넷그룹으로 작업하는 경우 다음 작업을 수행할 수 있습니다.

- 'vserver export-policy netgroup check-membership' 명령을 사용하여 클라이언트 IP가 특정 넷그룹의 구성원인지 여부를 확인할 수 있습니다.
- 'vserver services name-service getxxbyy netgrp' 명령을 사용하여 클라이언트가 넷그룹에 속하는지 확인할 수 있습니다.

  조회를 수행하는 기본 서비스는 구성된 이름 서비스 스위치 순서에 따라 선택됩니다.

ONTAP NFS SVM의 URI에서 넷그룹 로드

내보내기 정책 규칙에서 클라이언트를 일치시키는 데 사용할 수 있는 방법 중 하나는 netgroup에 나열된 호스트를 사용하는 것입니다. 외부 이름 서버에 저장된 넷그룹을 사용하는 대신 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다('vserver services name-service netgroup load').

시작하기 전에

넷그룹 파일은 SVM에 로드되기 전에 다음 요구 사항을 충족해야 합니다.

- 파일은 NIS를 채우는 데 사용되는 것과 동일한 적절한 넷그룹 텍스트 파일 형식을 사용해야 합니다.

  ONTAP는 넷그룹 텍스트 파일 형식을 로드하기 전에 검사합니다. 파일에 오류가 있으면 로드되지 않고 파일에서 수행해야 하는 수정 사항을 나타내는 메시지가 표시됩니다. 오류를 해결한 후 Netgroup 파일을 지정된 SVM에 다시 로드할 수 있습니다.

- 넷그룹 파일의 호스트 이름에 있는 모든 영문자는 소문자여야 합니다.
- 지원되는 최대 파일 크기는 5MB입니다.
- 네스팅 넷그룹에 대해 지원되는 최대 수준은 1000입니다.
- 넷그룹 파일에 호스트 이름을 정의할 때는 운영 DNS 호스트 이름만 사용할 수 있습니다.

  내보내기 액세스 문제를 방지하려면 DNS CNAME 또는 라운드 로빈 레코드를 사용하여 호스트 이름을 정의하면 안 됩니다.

- 넷그룹 파일에서 3중 그룹의 사용자 및 도메인 부분은 ONTAP에서 지원하지 않으므로 비워 두어야 합니다.

  호스트/IP 부분만 지원됩니다.

이 작업에 대해

ONTAP는 로컬 넷그룹 파일에 대한 호스트 별 검색을 지원합니다. 넷그룹 파일을 로드하면 ONTAP에서 자동으로 netgroup.byhost 맵을 생성하여 넷그룹 기준 호스트 검색을 설정합니다. 이렇게 하면 내보내기 정책 규칙을 처리하여 클라이언트 액세스를 평가할 때 로컬 넷그룹 검색 속도를 크게 높일 수 있습니다.

단계

1. URI를 통해 넷그룹을 SVM에 로드:

   'vserver services name-service netgroup load-vserver_vserver_name_-source{ftp|http|FTPS|https}://*Uri*'

넷그룹 파일을 로드하고 넷그룹을 생성합니다. byhost 맵은 몇 분 정도 걸릴 수 있습니다.

넷그룹을 업데이트하려면 파일을 편집하고 업데이트된 넷그룹 파일을 SVM에 로드할 수 있습니다.

예

다음 명령을 실행하면 HTTP URL 'http://intranet/downloads/corp-netgroup`: 에서 이름이 VS1 인 SVM에 넷그룹 정의가 로드됩니다

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ONTAP NFS SVM 넷그룹 정의 확인

SVM에 넷그룹을 로드한 후 'vserver services name-service netgroup status' 명령을 사용하여 넷그룹 정의의 상태를 확인할 수 있습니다. 이렇게 하면 SVM을 백업하는 모든 노드에서 넷그룹 정의가 일관되는지 확인할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 넷그룹 정의의 상태를 확인합니다.

   'vserver services name-service netgroup status'

   자세한 보기에 추가 정보를 표시할 수 있습니다.

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예

권한 수준을 설정한 후 다음 명령을 실행하면 모든 SVM에 대한 넷그룹 상태가 표시됩니다.

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

ONTAP NFS SVM에 대한 **NIS** 도메인 구성 생성

사용자 환경에서 NIS(Network Information Service)를 사용하여 이름 서비스를 제공하는 경우 'vserver services name-service NIS-domain create' 명령을 사용하여 SVM에 대한 NIS 도메인 구성을 생성해야 합니다.

시작하기 전에

SVM에서 NIS 도메인을 구성하기 전에 구성된 모든 NIS 서버를 사용할 수 있고 연결할 수 있어야 합니다.

NIS를 사용하여 디렉터리 검색을 수행할 경우 NIS 서버의 맵에는 각 항목에 대해 1,024자를 초과할 수 없습니다. 이 제한을 준수하지 않는 NIS 서버를 지정하지 마십시오. 그렇지 않으면 NIS 항목에 종속된 클라이언트 액세스가 실패할 수 있습니다.

이 작업에 대해

NIS 데이터베이스에 netgroup.byhost 맵이 포함되어 있으면 ONTAP에서 이를 사용하여 더 빨리 검색할 수 있습니다. 클라이언트 액세스 문제를 방지하려면 디렉토리의 netgroup.byhost 및 netgroup 맵을 항상 동기화해야 합니다. ONTAP 9.7부터 NIS 넷그룹.byhost 항목은 vserver services name-service NIS-domain netgroup-database 명령을 사용하여 캐싱될 수 있습니다.

호스트 이름 확인에 NIS를 사용하는 것은 지원되지 않습니다.

단계

1. NIS 도메인 구성 생성:

```
vserver services name-service nis-domain create -vserver vs1 -domain
<domain_name> -nis-servers <IP_addresses>
```

NIS 서버는 최대 10개까지 지정할 수 있습니다.

> 그만큼 `-nis-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-nis-servers` NIS 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

2. 도메인이 생성되었는지 확인합니다.

   'vserver services name-service NIS-domain show'를 참조하십시오

예

다음 명령을 실행하면 NIS 도메인용 NIS 도메인 구성이 생성됩니다. SVM은 IP 주소의 NIS `nisdomain` 서버로 이름이 `vs1` 지정됩니다. `192.0.2.180`

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

LDAP를 사용합니다

ONTAP NFS SVM에서 **LDAP** 이름 서비스 사용에 대해 알아보세요

환경에서 LDAP를 네임 서비스로 사용하는 경우 LDAP 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 LDAP 클라이언트로 설정해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 Active Directory 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. 이름 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 활성화하려면 LDAP 클라이언트 modify 명령에 '-try-channel-binding' 매개 변수를 사용합니다.

자세한 내용은 을 참조하십시오"Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

- ONTAP용 LDAP를 구성하기 전에 사이트 배포가 LDAP 서버 및 클라이언트 구성에 대한 모범 사례를 충족하는지 확인해야 합니다. 특히 다음 조건을 충족해야 합니다.
  - LDAP 서버의 도메인 이름이 LDAP 클라이언트의 항목과 일치해야 합니다.
  - LDAP 서버에서 지원하는 LDAP 사용자 암호 해시 유형에는 ONTAP에서 지원하는 해시 유형이 포함되어야 합니다.
    - 암호화(모든 유형) 및 SHA-1(SHA, SSHA).
    - ONTAP 9.8부터 SHA-2 해시(SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, SSHA-512)도 지원됩니다.
  - LDAP 서버에 세션 보안 조치가 필요한 경우 LDAP 클라이언트에서 이를 구성해야 합니다.

    다음 세션 보안 옵션을 사용할 수 있습니다.

    - LDAP 서명(데이터 무결성 검사 제공) 및 LDAP 서명 및 봉인(데이터 무결성 검사 및 암호화 제공)

        - TLS를 시작합니다
        - LDAPS(TLS 또는 SSL을 통한 LDAP)
    - 서명되고 봉인된 LDAP 쿼리를 사용하려면 다음 서비스를 구성해야 합니다.
        - LDAP 서버는 GSSAPI(Kerberos) SASL 메커니즘을 지원해야 합니다.
        - LDAP 서버에는 DNS 서버에 설정된 PTR 레코드와 DNS A/AAAA 레코드가 있어야 합니다.
        - Kerberos 서버는 DNS 서버에 SRV 레코드가 있어야 합니다.
    - 시작 TLS 또는 LDAPS를 활성화하려면 다음 사항을 고려해야 합니다.
        - LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.
        - LDAPS를 사용하는 경우 ONTAP 9.5 이상에서 TLS 또는 SSL에 대해 LDAP 서버를 활성화해야 합니다. SSL은 ONTAP 9.0-9.4에서 지원되지 않습니다.
        - 도메인에 인증서 서버가 이미 구성되어 있어야 합니다.
    - ONTAP 9.5 이상에서 LDAP 조회 추적을 활성화하려면 다음 조건을 충족해야 합니다.
        - 두 도메인은 다음 신뢰 관계 중 하나로 구성해야 합니다.
            - 양방향
            - 원웨이 - 프라이머리(primary)가 추천 도메인을 신뢰하는 곳입니다
            - 부모-자식
        - DNS는 참조된 모든 서버 이름을 확인하도록 구성되어야 합니다.
        - 도메인 암호는 -bind-as-cifs-server가 true로 설정된 경우 인증하기 위해 동일해야 합니다.

> LDAP 조회 추적에는 다음 구성이 지원되지 않습니다.
>
> - 모든 ONTAP 버전:
>   - 관리 SVM의 LDAP 클라이언트
> - ONTAP 9.8 및 이전 버전(9.9.1 이상에서 지원됨):
>   - LDAP 서명 및 봉인('-session-security' 옵션)
>   - 암호화된 TLS 연결('-use-start-tls' 옵션)
>   - LDAPS 포트 636을 통한 통신('-use-ldaps-for-ad-ldap' 옵션)

- SVM에서 LDAP 클라이언트를 구성할 때 LDAP 스키마를 입력해야 합니다.

  대부분의 경우 기본 ONTAP 스키마 중 하나가 적합합니다. 그러나 사용자 환경의 LDAP 스키마가 이러한 스키마와 다른 경우 LDAP 클라이언트를 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다. 사용자 환경의 요구 사항에 대해서는 LDAP 관리자에게 문의하십시오.

- 호스트 이름 확인에 LDAP를 사용하는 것은 지원되지 않습니다.

를 참조하십시오

- "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"
- "ONTAP SMB SVM에 자체 서명된 루트 CA 인증서를 설치합니다"

ONTAP NFS SVM에 대한 새 **LDAP** 클라이언트 스키마 생성

사용자 환경의 LDAP 스키마가 ONTAP 기본값과 다른 경우 LDAP 클라이언트 구성을 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2012 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

기본값이 아닌 LDAP 스키마를 사용해야 하는 경우 LDAP 클라이언트 구성을 생성하기 전에 만들어야 합니다. 새 스키마를 만들기 전에 LDAP 관리자에게 문의하십시오.

ONTAP에서 제공하는 기본 LDAP 스키마는 수정할 수 없습니다. 새 스키마를 만들려면 복사본을 만든 다음 복사본을 적절하게 수정합니다.

단계

1. 기존 LDAP 클라이언트 스키마 템플릿을 표시하여 복사할 템플릿을 식별합니다.

   'vserver services name-service ldap client schema show'를 참조하십시오

2. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

3. 기존 LDAP 클라이언트 스키마의 복사본을 만듭니다.

   'vserver services name-service LDAP 클라이언트 스키마 복사 - vserver_vserver_name_-schema_existing_schema_name_-new-schema-name_new_schema_name_'

4. 새 스키마를 수정하고 사용자 환경에 맞게 사용자 지정합니다.

   'vserver services name-service LDAP 클라이언트 스키마 수정

5. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP NFS 액세스를 위한 **LDAP** 클라이언트 구성 생성

ONTAP가 사용자 환경의 외부 LDAP 또는 Active Directory 서비스에 액세스하도록 하려면 먼저 스토리지 시스템에서 LDAP 클라이언트를 설정해야 합니다.

시작하기 전에

Active Directory 도메인 확인됨 목록의 처음 세 개 서버 중 하나가 작동 중이고 데이터를 제공하고 있어야 합니다. 그렇지 않으면 이 작업이 실패합니다.

여러 대의 서버가 있으며 그 중 어느 시점에서든 3대 이상의 서버가 다운됩니다.

단계

1. "vserver services name-service ldap client create" 명령에 대한 적절한 구성 값을 확인하려면 LDAP 관리자에게 문의하십시오.

   a. LDAP 서버에 대한 도메인 기반 또는 주소 기반 연결을 지정합니다.

      AD-DOMAIN과 -SERS 옵션은 상호 배타적입니다.

      - Active Directory 도메인에서 LDAP 서버 검색을 설정하려면 '-ad-domain' 옵션을 사용합니다.
        - 를 사용할 수 있습니다 `-restrict-discovery-to-site` LDAP 서버 검색을 지정된 도메인의 CIFS 기본 사이트로 제한하는 옵션입니다. 이 옵션을 사용하는 경우 에서 CIFS 기본 사이트도 지정해야 합니다 `-default-site`.
      - '-preferred-ad-servers' 옵션을 사용하여 쉼표로 구분된 목록에서 IP 주소로 하나 이상의 기본 Active Directory 서버를 지정할 수 있습니다. 클라이언트를 생성한 후 'vserver services name-service ldap client modify' 명령을 사용하여 이 목록을 수정할 수 있습니다.
      - 를 사용합니다 `-servers` 쉼표로 구분된 목록의 IP 주소로 하나 이상의 LDAP 서버(Active Directory 또는 UNIX)를 지정하는 옵션입니다.

        은 더 이상 사용되지 않습니다. `-ldap-servers` 필드는 다음을 대체합니다. `-servers` 필드. 이 필드에는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

   b. 기본 또는 사용자 지정 LDAP 스키마를 지정합니다.

      대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 읽기 전용 스키마를 사용할 수 있습니다. 그렇지 않으면 기본 스키마를 사용하는 것이 좋습니다. 이 경우 기본 스키마(읽기 전용)를 복사한 다음 복사본을 수정하여 고유한 스키마를 만들 수 있습니다.

      기본 스키마:

      - MS-AD-BIS

        RFC-2307bis를 기반으로 하는 이 방식은 대부분의 표준 Windows 2012 이상 LDAP 구축에 선호되는 LDAP 스키마입니다.

      - AD-IDMU

        UNIX용 Active Directory ID 관리를 기반으로 하는 이 스키마는 대부분의 Windows 2008, Windows 2012 이상 AD 서버에 적합합니다.

      - AD-SFU

        UNIX용 Active Directory 서비스를 기반으로 하는 이 스키마는 대부분의 Windows 2003 및 이전 AD 서버에 적합합니다.

      - RFC-2307

        RFC-2307(*LDAP*를 네트워크 정보 서비스로 사용하는 접근 방식)에 따라 이 스키마는 대부분의 UNIX AD 서버에 적합합니다.

c. 바인딩 값을 선택합니다.

- '-min-bind-level{anonymous|simple|sasl}'은 최소 bind authentication level을 지정한다.

  기본값은 ' * anonymous * '입니다.

- '-bind-dn_ldap_DN_'은 바인딩 사용자를 지정합니다.

  Active Directory 서버의 경우 계정(domain\user) 또는 보안 주체(user@domain.com) 양식에서 사용자를 지정해야 합니다. 그렇지 않으면 고유 이름(CN=user, DC=domain, DC=com) 형식으로 사용자를 지정해야 합니다.

- '-BIND-PASSWORD_PASSWORD_'는 바인딩 암호를 지정합니다.

d. 필요한 경우 세션 보안 옵션을 선택합니다.

LDAP 서버에서 필요한 경우 LDAP 서명 및 봉인 또는 TLS를 통한 LDAP를 활성화할 수 있습니다.

- '--세션-보안{none|sign|seal}'

  서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

  또한 서명과 봉인 바인딩이 실패할 경우 바인딩 인증을 ' * anonymous * ' 또는 ' * simple * '로 되돌리지 않으려면 '-min-bind-level' {'s ASL'}을 설정해야 합니다.

- '-use-start-tls'{'true'|'false'}

  '* true*'로 설정되어 있고 LDAP 서버가 이를 지원하는 경우 LDAP 클라이언트는 서버에 암호화된 TLS 연결을 사용합니다. 기본값은 ' * FALSE * '입니다. 이 옵션을 사용하려면 LDAP 서버의 자체 서명된 루트 CA 인증서를 설치해야 합니다.

> ⓘ 스토리지 VM에 도메인에 추가된 SMB 서버가 있고 LDAP 서버가 SMB 서버의 홈 도메인의 도메인 컨트롤러 중 하나인 경우 을 수정할 수 있습니다 `-session-security-for-ad-ldap` 옵션을 선택합니다 `vserver cifs security modify` 명령.

e. 포트, 쿼리 및 기준 값을 선택합니다.

기본값을 사용하는 것이 좋지만 LDAP 관리자에게 해당 값이 사용자 환경에 적합한지 확인해야 합니다.

- '-port_port_'는 LDAP 서버 포트를 지정합니다.

  기본값은 389입니다.

Start TLS를 사용하여 LDAP 연결을 보호하려면 기본 포트 389를 사용해야 합니다. 시작 TLS는 LDAP 기본 포트 389를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다. 포트를 변경하면 Start TLS가 실패합니다.

- '-query-timeout_integer_'는 쿼리 시간 제한(초)을 지정합니다.

  허용 범위는 1 ~ 10초입니다. 기본값은 3초입니다.

- `-base-dn_ldap_dn_'은 기본 DN을 지정합니다.

필요한 경우 여러 값을 입력할 수 있습니다(예: LDAP 조회 추적을 사용하는 경우). 기본값은 ""(root)입니다.

- '-base-scope'{'base'|'onelel'|'ubtree'}는 기본 검색 범위를 지정합니다.

  기본값은 'Subtree'입니다.

- '-referral-enabled'{'true'|'false'}는 LDAP 조회 추적 활성화 여부를 지정합니다.

  ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에 반환되어 원하는 레코드가 참조된 LDAP 서버에 있음을 나타내는 경우 ONTAP LDAP 클라이언트가 다른 LDAP 서버에 조회 요청을 참조할 수 있습니다. 기본값은 ' * FALSE * '입니다.

참조된 LDAP 서버에 있는 레코드를 검색하려면 LDAP 클라이언트 구성의 일부로 참조된 레코드의 기본 dn을 기본 dn에 추가해야 합니다.

2. 스토리지 VM에서 LDAP 클라이언트 구성을 생성합니다.

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

LDAP 클라이언트 구성을 생성할 때 스토리지 VM 이름을 제공해야 합니다.

3. LDAP 클라이언트 구성이 성공적으로 생성되었는지 확인합니다.

   'vserver services name-service ldap client show-client-config client_config_name'

예

다음 명령을 실행하면 스토리지 VM VS1이 LDAP용 Active Directory 서버와 함께 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

다음 명령을 실행하면 스토리지 VM VS1이 Active Directory 서버와 작동하여 서명과 봉인이 필요한 LDAP에 대해 ldap1이라는 새 LDAP 클라이언트 구성이 생성되고 LDAP 서버 검색이 지정된 도메인의 특정 사이트로 제한됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

다음 명령을 실행하면 스토리지 VM VS1이 LDAP 조회 추적이 필요한 LDAP용 Active Directory 서버와 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

다음 명령을 실행하면 기본 DN을 지정하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

다음 명령을 실행하면 조회 추적을 활성화하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

ONTAP NFS SVM과 **LDAP** 클라이언트 구성 연결

SVM에서 LDAP를 활성화하려면 "vserver services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결해야 합니다.

시작하기 전에

- LDAP 도메인은 네트워크 내에 이미 존재해야 하며 SVM이 있는 클러스터에서 액세스할 수 있어야 합니다.
- SVM에 LDAP 클라이언트 구성이 있어야 합니다.

단계

1. SVM에서 LDAP 지원:

   'vserver services name-service LDAP create-vserver_vserver_name_-client-config_client_config_name_'

그만큼 `vserver services name-service ldap create` 명령은 자동 구성 검증을 수행하고 ONTAP 이름 서버에 접속할 수 없는 경우 오류 메시지를 보고합니다.

다음 명령을 실행하면 "VS1" SVM에서 LDAP를 활성화하고 "ldap1" LDAP 클라이언트 구성을 사용하도록 구성합니다.

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. vserver services name-service ldap check 명령을 사용하여 이름 서버의 상태를 확인합니다.

   다음 명령은 SVM VS1 에서 LDAP 서버의 유효성을 검사합니다.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                  |
```

ONTAP NFS SVM에 대한 **LDAP** 소스 확인

SVM을 위한 네임 서비스 스위치 테이블에 네임 서비스에 대한 LDAP 소스가 올바르게 나열되어 있는지 확인해야 합니다.

단계

1. 현재 이름 서비스 스위치 테이블 내용을 표시합니다.

   'vserver services name-service ns-switch show -vserver_svm_name_'

   다음 명령을 실행하면 SVM My_SVM의 결과가 표시됩니다.

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

이름 매핑 정보를 검색할 소스 및 순서를 지정합니다. UNIX 전용 환경에서는 이 항목이 필요하지 않습니다. 이름 매핑은 UNIX와 Windows를 모두 사용하는 혼합 환경에서만 필요합니다.

2. 필요에 따라 ns-switch 항목을 업데이트합니다.

ns-switch 항목을 업데이트하려면...	명령 입력...
사용자 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database passwd - sources ldap, files'
그룹 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database group-sources ldap, files'
넷그룹 정보입니다	'vserver services name-service ns-switch modify -vserver_vserver_name_-database 넷그룹 - 소스 LDAP, 파일

강력한 보안을 위해 **NFS**와 **Kerberos** 사용

보안 인증을 위해 **ONTAP NFS**와 함께 **Kerberos**를 사용하는 방법에 대해 알아보세요**.**

Kerberos가 강력한 인증을 위해 사용자 환경에서 사용되는 경우 Kerberos 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 Kerberos 클라이언트로 사용하도록 설정해야 합니다.

환경은 다음 지침을 충족해야 합니다.

- ONTAP용 Kerberos를 구성하기 전에 Kerberos 서버 및 클라이언트 구성에 대한 모범 사례를 따라야 합니다.
- 가능하면 Kerberos 인증이 필요한 경우 NFSv4 이상을 사용합니다.

  NFSv3은 Kerberos와 함께 사용할 수 있습니다. 하지만 Kerberos의 모든 보안 이점은 NFSv4 이상의 ONTAP 구축에서만 실현됩니다.

- 중복 서버 액세스를 프로모션하려면 Kerberos가 동일한 SPN을 사용하여 클러스터의 여러 노드에 있는 여러 데이터 LIF에서 활성화되어야 합니다.
- SVM에서 Kerberos를 사용하도록 설정할 경우 NFS 클라이언트 구성에 따라 볼륨 또는 qtree의 내보내기 규칙에 다음 보안 방법 중 하나를 지정해야 합니다.
  - "krb5"(Kerberos v5 프로토콜)
  - "krb5i"(체크섬을 사용한 무결성 검사를 포함한 Kerberos v5 프로토콜)
  - "krb5p"(개인정보 보호 서비스가 있는 Kerberos v5 프로토콜)

Kerberos 서버 및 클라이언트 외에도 ONTAP가 Kerberos를 지원하도록 다음과 같은 외부 서비스를 구성해야 합니다.

- 디렉터리 서비스

  SSL/TLS를 통해 LDAP를 사용하도록 구성된 Active Directory 또는 OpenLDAP와 같은 환경에서 보안 디렉터리 서비스를 사용해야 합니다. 요청이 일반 텍스트로 전송되므로 안전하지 않은 NIS를 사용하지 마십시오.

- NTP

  NTP를 실행하는 작업 시간 서버가 있어야 합니다. 시간 편중이 발생하여 Kerberos 인증 실패를 방지하려면 이 작업이 필요합니다.

- 도메인 이름 확인(DNS)

  각 UNIX 클라이언트와 각 SVM LIF에는 정방향 및 역방향 조회 영역에서 KDC에 등록된 적절한 서비스 레코드(SRV)가 있어야 합니다. 모든 참가자는 DNS를 통해 제대로 확인할 수 있어야 합니다.

ONTAP SVM에서 **NFS Kerberos** 구성에 대한 **UNIX** 권한 확인

Kerberos를 사용하려면 SVM 루트 볼륨 및 로컬 사용자 및 그룹에 대해 특정 UNIX 사용 권한을 설정해야 합니다.

단계

1. SVM 루트 볼륨에 대한 관련 권한을 표시합니다.

   'volume show-volume_root_vol_name_-fields user, group, unix-permissions

   SVM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름...	설정 중...
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	755

   이 값이 표시되지 않으면 볼륨 수정 명령을 사용하여 값을 업데이트합니다.

2. 로컬 UNIX 사용자를 표시합니다.

'vserver services name-service unix-user show -vserver_vserver_name_'

SVM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 **ID**입니다	기본 그룹 **ID**입니다	설명
NFS 를 참조하십시오	500입니다	0	GSS INIT 단계에 필요함. NFS 클라이언트 사용자 SPN의 첫 번째 구성 요소가 사용자로 사용됩니다. NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다.
루트	0	0	마운팅에 필요합니다.

이러한 값이 표시되지 않으면 'vserver services name-service unix-user modify' 명령을 사용하여 해당 값을 업데이트할 수 있습니다.

3. 로컬 UNIX 그룹을 표시합니다.

   'vserver services name-service unix-group show -vserver_vserver__name'

   SVM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 **ID**입니다
데몬	1
루트	0

이러한 값이 표시되지 않으면 'vserver services name-service unix-group modify' 명령을 사용하여 해당 값을 업데이트할 수 있습니다.

ONTAP SVM에서 **NFS Kerberos** 영역 구성 만들기

ONTAP가 사용자 환경에서 외부 Kerberos 서버에 액세스하도록 하려면 먼저 기존 Kerberos 영역을 사용하도록 SVM을 구성해야 합니다. 이렇게 하려면 Kerberos KDC 서버에 대한 구성 값을 수집한 다음 "vserver NFS Kerberos realm create" 명령을 사용하여 SVM에서 Kerberos 영역 구성을 생성해야 합니다.

시작하기 전에

클러스터 관리자는 인증 문제를 방지하기 위해 스토리지 시스템, 클라이언트 및 KDC 서버에서 NTP를 구성해야 합니다. 클라이언트와 서버 간의 시간 차이(클럭 편중)는 인증 실패의 일반적인 원인입니다.

단계

1. Kerberos 관리자에게 문의하여 "vserver NFS Kerberos realm create" 명령을 제공하는 적절한 구성 값을 확인하십시오.
2. SVM에서 Kerberos 영역 구성 생성:

   "vserver NFS Kerberos 영역 create -vserver_vserver_name_
   -realm_realm_name__{AD_KDC_server_values|AD_KDC_server_values}_-comment "*text*"

3. Kerberos 영역 구성이 성공적으로 생성되었는지 확인합니다.

   가상 NFS Kerberos 영역 표시

예

다음 명령을 실행하면 Microsoft Active Directory 서버를 KDC 서버로 사용하는 SVM VS1 용 NFS Kerberos 영역 구성이 생성됩니다. Kerberos 영역은 AUTH.EXAMPLE.COM 입니다. Active Directory 서버의 이름은 ad-1이고 IP 주소는 10.10.8.14입니다. 허용되는 시간 편중은 300초(기본값)입니다. KDC 서버의 IP 주소는 10.10.8.14이고 포트 번호는 88(기본값)입니다. "Microsoft Kerberos 구성"이 주석입니다.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

다음 명령을 실행하면 MIT KDC를 사용하는 SVM VS1 용 NFS Kerberos 영역 구성이 생성됩니다. Kerberos 영역은 SECURITY.EXAMPLE.COM 입니다. 허용되는 시간 편중은 300초입니다. KDC 서버의 IP 주소는 10.10.9.1이고 포트 번호는 88입니다. KDC 공급업체는 UNIX 공급업체를 나타내는 기타 벤더입니다. 관리 서버의 IP 주소는 10.10.9.1이고 포트 번호는 749(기본값)입니다. 암호 서버의 IP 주소는 10.10.9.1이고 포트 번호는 464(기본값)입니다. "UNIX Kerberos 구성"이 주석입니다.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

ONTAP SVM에 대해 **NFS Kerberos** 허용 암호화 유형 구성

기본적으로 ONTAP는 NFS Kerberos인 DES, 3DES, AES-128, AES-256에 대해 다음 암호화 유형을 지원합니다. "vserver nfs modify" 명령을 `-enc-types' 매개 변수와 함께 사용하면 각 SVM에 대해 허용된 암호화 유형을 특정 환경의 보안 요구사항에 맞게 구성할 수 있습니다.

이 작업에 대해

클라이언트 호환성을 극대화하기 위해 ONTAP는 기본적으로 약한 DES와 강력한 AES 암호화를 모두 지원합니다. 예를 들어, 보안을 강화하려는 경우 사용자 환경에서 이 절차를 사용하여 DES 및 3DES를 비활성화하고 클라이언트가 AES

암호화만 사용하도록 할 수 있습니다.

사용 가능한 가장 강력한 암호화를 사용해야 합니다. ONTAP의 경우, AES-256입니다. 해당 환경에서 이 암호화 수준이 지원되는지 KDC 관리자에게 확인해야 합니다.

- SVM에서 AES를 완전히 활성화 또는 비활성화(AES-128 및 AES-256 모두)하면 원래의 DES 기본/키탭 파일이 삭제되므로 SVM을 위한 모든 LIF에서 Kerberos 구성을 비활성화해야 합니다.

  이를 변경하기 전에 NFS 클라이언트가 SVM에서 AES 암호화를 사용하지 않는지 확인해야 합니다.

- DES 또는 3DES를 활성화 또는 비활성화할 경우 LIF에서 Kerberos 구성을 변경할 필요가 없습니다.

단계

1. 허용되는 암호화 유형을 사용하거나 사용하지 않도록 설정합니다.

활성화 또는 비활성화하려는 경우...	다음 단계를 따르십시오...
DES 또는 3DES입니다	a. SVM의 NFS Kerberos 허용 암호화 유형을 구성합니다. + 'vserver NFS modify -vserver_vserver_name_-enc -types_encryption_types_' 여러 암호화 유형을 쉼표로 구분합니다. b. 성공적으로 변경되었는지 확인합니다. + 'vserver nfs show -vserver_vserver_name_ -fields fitted-enc-types'

활성화 또는 비활성화하려는 경우...	다음 단계를 따르십시오...
AES-128 또는 AES-256	a. SVM 및 LIF Kerberos 사용 설정 식별: + 'vserver NFS Kerberos interface show b. NFS Kerberos에서 허용할 암호화 유형을 수정하려는 SVM의 모든 LIF에서 Kerberos를 해제합니다. + 'vserver NFS Kerberos interface disable-lif_lif_name_' c. SVM의 NFS Kerberos 허용 암호화 유형을 구성합니다. + 'vserver NFS modify -vserver_vserver_name_-enc -types_encryption_types_' 여러 암호화 유형을 쉼표로 구분합니다. d. 성공적으로 변경되었는지 확인합니다. + 'vserver nfs show -vserver_vserver_name_ -fields fitted-enc-types' e. SVM의 모든 LIF에서 Kerberos를 사용하도록 다시 설정합니다. + 'vserver NFS Kerberos interface enable-lif_lif_name_-spN_service_principal_name_' f. 모든 LIF에서 Kerberos가 설정되어 있는지 확인합니다. + "vserver NFS Kerberos interface show

ONTAP LIF에서 **NFS Kerberos** 활성화

데이터 LIF에서 Kerberos를 사용하도록 설정하려면 'vserver NFS Kerberos interface enable' 명령을 사용하십시오. 그러면 SVM에서 NFS에 Kerberos 보안 서비스를 사용할 수 있습니다.

이 작업에 대해

Active Directory KDC를 사용하는 경우 사용되는 SPN의 처음 15자는 영역 또는 도메인 내의 SVM에서 고유해야 합니다.

단계

1. NFS Kerberos 구성 생성:

   'vserver NFS Kerberos interface enable-vserver_vserver_name_-lif_logical_interface_-spN_service_principal_name_'

   ONTAP에서 Kerberos 인터페이스를 활성화하려면 KDC의 SPN에 대한 암호 키가 필요합니다.

   Microsoft KDC의 경우 KDC에 문의하고 CLI에서 사용자 이름 및 암호 프롬프트가 발급되어 비밀 키를 얻습니다. Kerberos 영역의 다른 OU에 SPN을 만들어야 하는 경우 선택적 '-ou' 매개 변수를 지정할 수 있습니다.

   비 Microsoft KDC의 경우 다음 두 가지 방법 중 하나를 사용하여 비밀 키를 얻을 수 있습니다.

만약...	다음 매개 변수도 명령에 포함해야 합니다.
KDC에서 직접 키를 검색하려면 KDC 관리자 자격 증명을 사용합니다	'-admin-username"*kdc_admin_username*'
KDC 관리자 자격 증명이 없지만 키가 포함된 KDC의 keytab 파일이 있습니다	'-keytab-Uri '{ftp

2. Kerberos가 LIF에서 설정되었는지 확인합니다.

   'vserver nfs Kerberos-config show'

3. 1단계와 2단계를 반복하여 여러 LIF에서 Kerberos를 사용하도록 설정합니다.

예

다음 명령을 실행하면 OU lab2ou 에서 SPN NFS /ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM 와 함께 논리 인터페이스 ves03-d1에서 이름이 VS1 인 SVM에 대한 NFS Kerberos 구성이 생성되고 확인됩니다.

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

NFS 지원 SVM에 스토리지 용량 추가

ONTAP NFS 지원 SVM에 스토리지 용량을 추가하는 방법에 대해 알아보세요.

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.

시작하기 전에

- 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.

ONTAP NFS 내보내기 정책 만들기

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
```

ONTAP NFS 내보내기 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.

시작하기 전에

- 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,…+
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.
"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

보안 유형을 다음으로 설정한 경우…	일치하는 클라이언트가 내보낸 데이터에 액세스할 수 있습니다…
'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.
엑스포트 정책에 대한 추가 규칙	a. 정책에 기존 규칙을 표시합니다. + 'vserver export-policy rule show-instance-policyname_your_policy_' 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

ONTAP NFS 볼륨 생성

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 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

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
```

ONTAP NFS qtree 생성

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

시작하기 전에

- 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 **ONTAP NFS** 액세스 보안에 대해 알아보세요.

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.

ONTAP NFS 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 **ONTAP NFS** 내보내기 정책 할당

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
```

ONTAP NFS 내보내기 정책을 **qtree**에 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.

시작하기 전에

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 **ONTAP NFS** 클라이언트 액세스를 확인하세요**.**

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 **ONTAP NFS** 액세스 테스트

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.

시작하기 전에

- 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_'

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

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.

추가 **ONTAP NFS** 정보를 찾을 수 있는 곳

NFS 클라이언트 액세스를 성공적으로 테스트한 후 추가 NFS 구성을 수행하거나 SAN 액세스를 추가할 수 있습니다. 프로토콜 액세스가 완료되면 SVM(스토리지 가상 머신)의 루트 볼륨을 보호해야 합니다.

NFS 구성

다음 정보 및 기술 보고서를 사용하여 NFS 액세스를 추가로 구성할 수 있습니다.

- "NFS 관리"

  NFS를 사용하여 파일 액세스를 구성 및 관리하는 방법에 대한 설명은 에 나와 있습니다.

- "NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"

  NFSv3 및 NFSv4 운영 가이드 역할을 하며 NFSv4를 중심으로 ONTAP 운영 체제에 대한 개요를 제공합니다.

- "NetApp 기술 보고서 4073: 안전한 통합 인증"

  NFS 스토리지 인증을 위한 UNIX 기반 Kerberos 버전 5(krb5) 서버 및 Windows Server Active Directory(AD)를 KDC 및 LDAP(Lightweight Directory Access Protocol) ID 공급자로 사용하도록 ONTAP를 구성하는 방법은 에 나와 있습니다.

- "NetApp 기술 보고서 3580: NFSv4 향상 및 모범 사례 가이드 Data ONTAP 구축"

  에서는 ONTAP를 실행하는 시스템에 접속된 AIX, Linux 또는 Solaris 클라이언트에서 NFSv4 구성 요소를 구축하는 동안 따라야 하는 Best Practice를 설명합니다.

네트워킹 구성

다음 정보 및 기술 보고서를 사용하여 네트워킹 기능 및 이름 서비스를 추가로 구성할 수 있습니다.

- "NFS 관리"

  에서는 ONTAP 네트워킹을 구성하고 관리하는 방법에 대해 설명합니다.

- "NetApp 기술 보고서 4182: 이더넷 스토리지 설계 고려사항 및 clustered Data ONTAP 구성에 대한 모범 사례"

  ONTAP 네트워크 구성의 구현을 설명하고 일반적인 네트워크 배포 시나리오 및 모범 사례 권장 사항을 제공합니다.

- "NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

  인증을 위해 LDAP, NIS, DNS 및 로컬 파일 구성을 구성하는 방법은 에 나와 있습니다.

SAN 프로토콜 구성

새 SVM에 대한 SAN 액세스를 제공하거나 수정하려는 경우 여러 호스트 운영 체제에서 사용할 수 있는 FC 또는 iSCSI 구성 정보를 사용할 수 있습니다.

루트 볼륨 보호

SVM에서 프로토콜을 구성한 후에는 루트 볼륨이 보호되는지 확인해야 합니다.

- "데이터 보호"

  NAS 지원 SVM에 대한 NetApp의 모범 사례인 SVM 루트 볼륨을 보호하기 위해 로드 공유 미러를 생성하는 방법에

대해 설명합니다. 또한, 로드 공유 미러에서 SVM 루트 볼륨을 프로모션하여 볼륨 장애 또는 손실로부터 빠르게 복구하는 방법을 설명합니다.

ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다릅니까

ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다릅니까

ONTAP에서 NFS 엑스포트를 구축하는 방법에 대한 생소한 사용자는 7-Mode와 ONTAP 엑스포트 구성 툴을 비교할 수 있을 뿐만 아니라 7-Mode '/etc/exports' 파일을 클러스터 정책 및 규칙과 비교할 수 있습니다.

ONTAP에는 '/etc/exports' 파일과 'exportfs' 명령이 없습니다. 대신 엑스포트 정책을 정의해야 합니다. 엑스포트 정책을 사용하면 7-Mode와 동일한 방식으로 클라이언트 액세스를 제어할 수 있으며, 여러 볼륨에 동일한 엑스포트 정책을 다시 사용할 수 있는 등 기능도 추가로 제공됩니다.

관련 정보

"NFS 관리"

"NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"

7-Mode 및 ONTAP NFS 내보내기 비교에 대해 알아보세요

ONTAP의 내보내기는 7-Mode 환경에 있는 내보내기와 다르게 정의 및 사용됩니다.

차이 영역	향상됩니다	ONTAP
내보내기 정의 방법	내보내기는 '/etc/exports' 파일에 정의되어 있습니다.	내보내기는 SVM 내에서 엑스포트 정책을 생성하여 정의합니다. SVM에는 둘 이상의 엑스포트 정책이 포함될 수 있습니다.
수출 범위	• 내보내기는 지정된 파일 경로 또는 qtree에 적용됩니다. • 각 파일 경로 또는 qtree에 대해 '/etc/exports'에 별도의 항목을 생성해야 합니다. • 내보내기는 '/etc/exports' 파일에 정의되어 있는 경우에만 지속적입니다.	• 엑스포트 정책은 볼륨에 포함된 모든 파일 경로 및 qtree를 포함하여 전체 볼륨에 적용됩니다. • 원하는 경우 둘 이상의 볼륨에 내보내기 정책을 적용할 수 있습니다. • 모든 내보내기 정책은 시스템을 다시 시작할 때마다 유지됩니다.

펜싱(동일한 리소스에 대한 특정 클라이언트에 대해 다른 액세스 지정)	내보낸 단일 리소스에 대해 특정 클라이언트에 서로 다른 액세스 권한을 제공하려면 각 클라이언트와 허용된 액세스 권한을 '/etc/exports' 파일에 나열해야 합니다.	엑스포트 정책은 다양한 개별 엑스포트 규칙으로 구성됩니다. 각 내보내기 규칙은 리소스에 대한 특정 액세스 권한을 정의하고 해당 권한이 있는 클라이언트를 나열합니다. 특정 클라이언트에 대해 다른 액세스를 지정하려면 각 특정 액세스 권한 집합에 대한 내보내기 규칙을 만들고 해당 권한이 있는 클라이언트를 나열한 다음 엑스포트 정책에 규칙을 추가해야 합니다.
이름 앨리어싱	내보내기를 정의할 때 파일 경로 이름과 내보내기 이름을 다르게 지정할 수 있습니다. '/etc/exports' 파일에서 해당 내보내기를 정의할 때 '-actual' 매개변수를 사용해야 합니다.	내보낸 볼륨의 이름을 실제 볼륨 이름과 다르게 설정할 수 있습니다. 이렇게 하려면 SVM 네임스페이스 내에서 사용자 지정 접합 경로 이름을 사용하여 볼륨을 마운트해야 합니다. 기본적으로 볼륨은 해당 볼륨 이름으로 마운트됩니다. 볼륨의 접합 경로 이름을 사용자 지정하려면 마운트를 해제하고 이름을 바꾼 다음 다시 마운트해야 합니다.

ONTAP NFS 내보내기 정책 예제에 대해 알아보세요

내보내기 정책의 예를 검토하여 ONTAP에서 내보내기 정책의 작동 방식을 보다 잘 이해할 수 있습니다.

7-Mode 내보내기의 ONTAP 구현 예

다음 예에서는 '/etc/export' 파일에 나타나는 7-Mode 내보내기를 보여 줍니다.

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

이 내보내기를 클러스터된 내보내기 정책으로 복제하려면 세 개의 엑스포트 규칙을 사용하여 엑스포트 정책을 생성한 다음 볼륨 vol1에 엑스포트 정책을 할당해야 합니다.

규칙	요소	값
규칙 1	'-clientmatch'(클라이언트 사양)	'@readonly_netgroup'

규칙	요소	값
'-ruleindex'(규칙 목록에 있는 내보내기 규칙의 위치)	"1"	'-프로토콜'
'NFS'입니다	'-rorule'(읽기 전용 액세스 허용)	Sys(AUTH_SYS로 인증받은 클라이언트)
'-rwrule'(읽기-쓰기 액세스 허용)	"안 돼.	'-superuser'(슈퍼유저 액세스 허용)
'없음'(root_squashed_to anon)	규칙 2	'-clientmatch'
'@rootaccess_netgroup'	룰레인덱스	2
'-프로토콜'	'NFS'입니다	'-rorule'
'스'입니다	'-rwrule'	'스'입니다
'-슈퍼유저'	'스'입니다	규칙 3
'-clientmatch'	'@readwrite_netgroup1, @readwrite_netgroup2'	룰레인덱스
3	'-프로토콜'	'NFS'입니다
'-rorule'	'스'입니다	'-rwrule'
'스'입니다	'-슈퍼유저'	"없음"

1. exp_vol1이라는 엑스포트 정책을 생성합니다.

   'vserver export-policy create-vserver NewSVM-policyname exp_vol1'

2. 기본 명령에 다음 매개 변수를 사용하여 세 개의 규칙을 생성합니다.
   - 기본 명령: + 'vserver export-policy rule create-vserver NewSVM-policyname exp_vol1'
   - 규칙 매개 변수: + ``clientmatch@readonly_netgroup-ruleindex 1-protocol nfs-rorule sys-rwrule never-superuser none'+'-clientmatch@rootaccess_netgroup-rindex 2-protocol nfs-rorule_rule_rule_rule -clientmatch@readwrite_wrule_wrule -rrulule_nfs -rrrrrrule_none
3. 볼륨 vol1에 정책을 할당합니다.

   'volume modify -vserver NewSVM-volume vol1-policy exp_vol1'

7-Mode 엑스포트 통합의 예

다음 예에서는 10개의 qtree당 한 줄이 포함된 7-Mode '/etc/export' 파일을 보여 줍니다.

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

ONTAP에서는 각 qtree에 대해 -clientmatch host1519s 등의 규칙이 있는 정책 또는 -clientmatch host2057s 등의 규칙이 있는 정책 중 하나가 필요합니다.

1. exp_vol1q1 및 exp_vol1q2라는 두 개의 엑스포트 정책을 생성합니다.
   - 'vserver export-policy create-vserver NewSVM-policyname exp_vol1q1'
   - 'vserver export-policy create-vserver NewSVM-policyname exp_vol1q2'
2. 각 정책에 대한 규칙 생성:
   - 'vserver export-policy rule create-vserver newSVM-policyname exp_vol1q1-clientmatch host1519s-rwrule sys-superuser sys'
   - 'vserver export-policy rule create-vserver newSVM-policyname exp_vol1q2-clientmatch host1519s-rwrule sys-superuser sys'
3. qtree에 정책을 적용합니다.
   - '볼륨 qtree modify -vserver NewSVM-qtree-path /vol/vol1/q_1472-export-policy exp_vol1q1'
   - [다음 4 qtree…]
   - '볼륨 qtree modify -vserver NewSVM-qtree-path /vol/vol1/q_2237 -export-policy exp_vol1q2'
   - [다음 4 qtree…]

나중에 이러한 호스트에 대해 추가 qtree를 추가해야 하는 경우 동일한 엑스포트 정책을 사용합니다.