멀티프로토콜 구성 워크플로우

System Manager Classic

NetApp
April 09, 2024

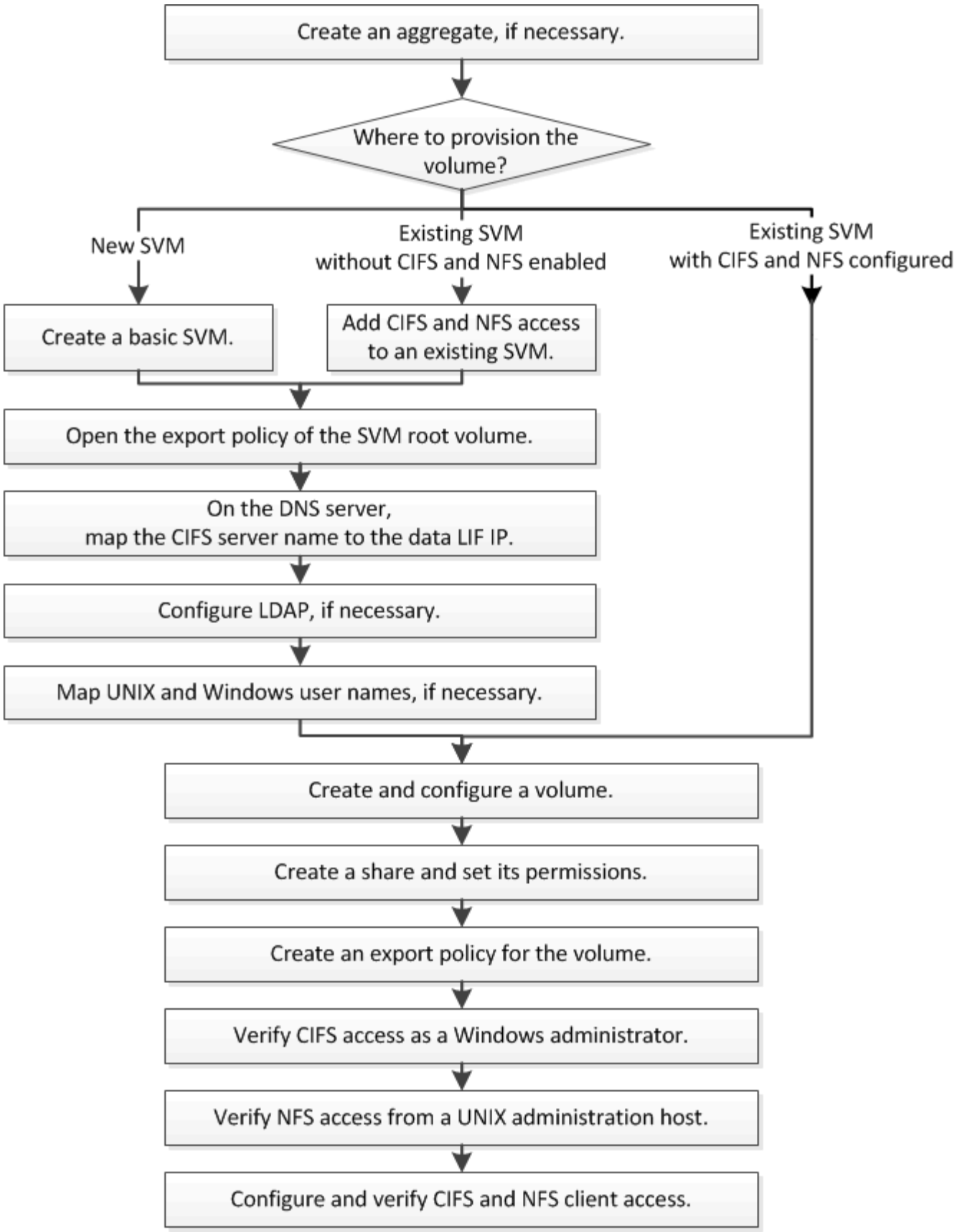
This PDF was generated from https://docs.netapp.com/ko-kr/ontap-sm-classic/nas-multiprotocol-config/task_creating_aggregate.html on April 09, 2024. Always check docs.netapp.com for the latest.

목차

멀티프로토콜 구성 워크플로우 1
Aggregate를 생성합니다 3
새 볼륨을 프로비저닝할 위치를 결정합니다 3
볼륨을 생성하고 구성합니다 17
공유를 생성하고 해당 권한을 설정합니다 18
볼륨에 대한 엑스포트 정책을 생성합니다 19
SMB 클라이언트 액세스를 확인합니다 20
UNIX 관리 호스트에서 NFS 액세스를 확인합니다 21
CIFS 및 NFS 클라이언트 액세스를 구성하고 확인합니다 22

멀티프로토콜 구성 워크플로우

SMB/CIFS와 NFS를 모두 구성하려면 선택적으로 애그리게이트를 생성하고, 새 SVM을 생성하거나, 기존 SVM을 구성하거나, 볼륨 생성, 공유 및 내보내기를 수행하고, UNIX 및 Windows 관리 호스트의 액세스를 확인해야 합니다. 그런 다음 SMB/CIFS 및 NFS 클라이언트에 대한 액세스를 열 수 있습니다.


Create an aggregate, if necessary.
Where to provision the volume?
New SVM
Existing SVM without CIFS and NFS enabled
Existing SVM with CIFS and NFS configured
Create a basic SVM.
Add CIFS and NFS access to an existing SVM.
Open the export policy of the SVM root volume.
On the DNS server, map the CIFS server name to the data LIF IP.
Configure LDAP, if necessary.
Map UNIX and Windows user names, if necessary.
Create and configure a volume.
Create a share and set its permissions.
Create an export policy for the volume.
Verify CIFS access as a Windows administrator.
Verify NFS access from a UNIX administration host.
Configure and verify CIFS and NFS client access.

Aggregate를 생성합니다

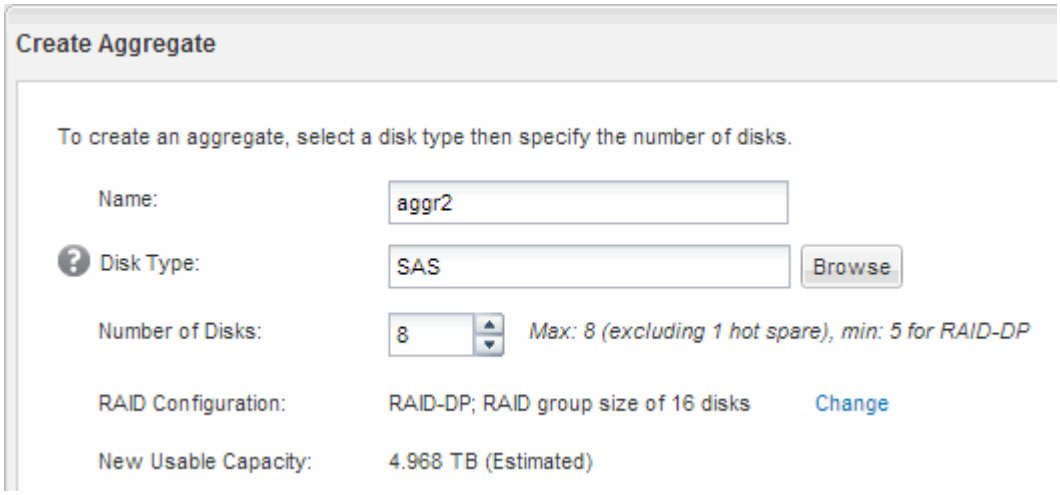
기존 Aggregate를 사용하지 않으려는 경우 새로운 Aggregate를 생성하여 프로비저닝 중인 볼륨에 물리적 스토리지를 제공할 수 있습니다.

이 작업에 대해

새 볼륨에 사용할 기존 Aggregate가 있는 경우 이 절차를 건너뛸 수 있습니다.

단계

1. 웹 브라우저에 URL 'https://IP-address-of-cluster-management-LIF` 를 입력하고 클러스터 관리자 자격 증명을 사용하여 System Manager에 로그인합니다.
2. 애그리게이트 * 창으로 이동합니다.
3. 생성 * 을 클릭합니다
4. 화면의 지시에 따라 기본 RAID-DP 구성을 사용하여 애그리게이트를 생성한 다음 * Create * 를 클릭합니다.



결과

Aggregate는 지정된 구성으로 생성되어 애그리게이트 창의 애그리게이트 목록에 추가됩니다.

새 볼륨을 프로비저닝할 위치를 결정합니다

새 멀티프로토콜 볼륨을 생성하기 전에 볼륨을 기존 SVM(스토리지 가상 머신)에 배치할지 여부와 필요한 경우 SVM에 필요한 구성의 크기를 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

절차를 참조하십시오

- 새 SVM에서 볼륨을 프로비저닝하고 싶은 경우, 기본 SVM을 생성합니다.

  "기본 SVM 생성"

  기존 SVM에서 CIFS 및 NFS가 아직 활성화되지 않은 경우 이 옵션을 선택해야 합니다.

- CIFS와 NFS를 모두 사용하도록 설정했지만 구성하지 않은 기존 SVM에서 볼륨을 프로비저닝하려는 경우 기존 SVM에 CIFS 및 NFS 액세스를 추가합니다.

  "기존 SVM에서 CIFS 및 NFS 액세스 추가"

- CIFS 및 NFS 멀티 프로토콜 액세스용으로 완전히 구성된 기존 SVM에서 볼륨을 프로비저닝하고 싶은 경우, 볼륨을 직접 생성 및 구성할 수 있습니다.

  "볼륨 생성 및 구성"

기본 **SVM**을 생성합니다

마법사를 사용하면 새 SVM(스토리지 가상 시스템) 생성, DNS(Domain Name System) 구성, LIF(데이터 논리 인터페이스) 생성, CIFS 서버 구성, NFS 활성화 및 NIS(옵션) 구성 프로세스를 안내합니다.

시작하기 전에

- 네트워크를 구성해야 하며 관련 물리적 포트를 네트워크에 연결해야 합니다.
- SVM에서 사용할 네트워킹 구성 요소는 무엇입니까?
  - 노드 및 해당 노드의 특정 포트에서 데이터 논리 인터페이스(LIF)가 생성됩니다
  - 데이터 LIF의 IP 주소를 프로비저닝할 서브넷 또는 선택적으로 데이터 LIF에 할당할 특정 IP 주소를 지정합니다
  - SVM을 추가하는 데 필요한 자격 증명과 함께 SVM이 연결할 Active Directory(AD) 도메인
  - NIS 정보 - 사이트에서 이름 서비스 또는 이름 매핑에 NIS를 사용하는 경우
- 서브넷은 NIS(Network Information Service), LDAP(Lightweight Directory Access Protocol), AD(Active Directory) 및 DNS와 같은 서비스에 필요한 모든 외부 서버로 라우팅할 수 있어야 합니다.
- 모든 외부 방화벽은 네트워크 서비스에 대한 액세스를 허용하도록 적절하게 구성되어야 합니다.
- AD 도메인 컨트롤러, 클라이언트 및 SVM의 시간은 서로 5분 이내에 서로 동기화해야 합니다.

이 작업에 대해

멀티프로토콜 액세스를 위해 SVM을 생성할 때 SVM(Storage Virtual Machine) 설정 창의 프로비저닝 섹션을 사용해서는 안 되며, 다중 프로토콜 액세스를 지원하는 단일 볼륨이 아닌 두 개의 볼륨을 생성합니다. 나중에 워크플로우에서 볼륨을 프로비저닝할 수 있습니다.

단계

1. SVM * 창으로 이동합니다.
2. 생성 * 을 클릭합니다
3. SVM(Storage Virtual Machine) 설정 * 대화 상자에서 SVM을 생성합니다.

   a. SVM의 고유한 이름을 지정합니다.

      이름은 FQDN(정규화된 도메인 이름)이거나 클러스터 전체에서 고유한 이름을 보장하는 다른 규칙을 따라야 합니다.

   b. 모든 프로토콜을 즉시 구성하지 않아도 라이센스가 있고 SVM에서 사용할 프로토콜을 모두 선택합니다.

c. 기본 언어 설정인 C. UTF-8을 유지합니다.

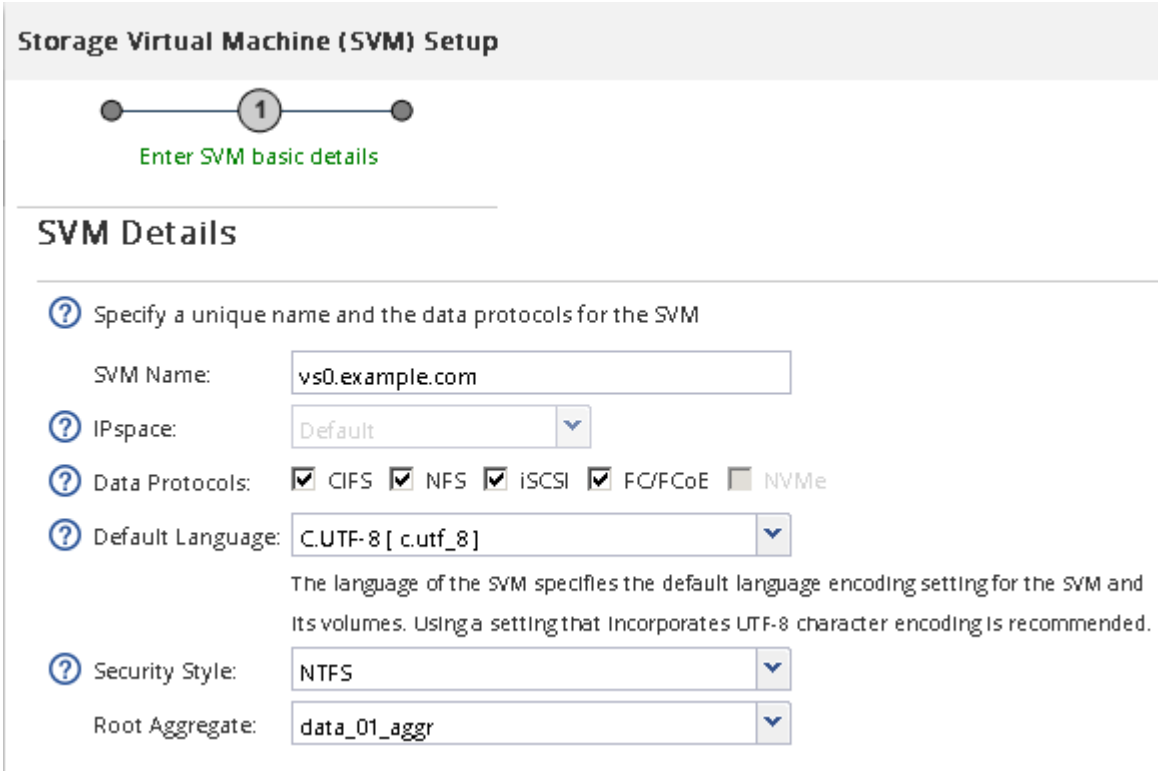
> NFS 및 SMB/CIFS 클라이언트 모두에서 국제 문자 표시를 지원하는 경우 ONTAP 9.5부터 사용할 수 있는 * UTF8MB4 * 언어 코드를 사용하는 것이 좋습니다.

d. * 선택 사항 *: 보안 스타일이 기본 설정으로 설정되어 있는지 확인하십시오.

   CIFS 프로토콜을 선택하면 기본적으로 보안 스타일이 NTFS로 설정됩니다.

e. * 선택 사항 *: SVM 루트 볼륨을 포함할 루트 애그리게이트를 선택합니다.

   루트 볼륨에 대해 선택한 aggregate에서 데이터 볼륨의 위치가 결정되지 않습니다. 데이터 볼륨의 애그리게이트는 이후 단계에서 별도로 선택됩니다.



f. * 선택 사항 *: * DNS Configuration * 영역에서 기본 DNS 검색 도메인과 네임 서버가 이 SVM에 사용할 것인지 확인합니다.

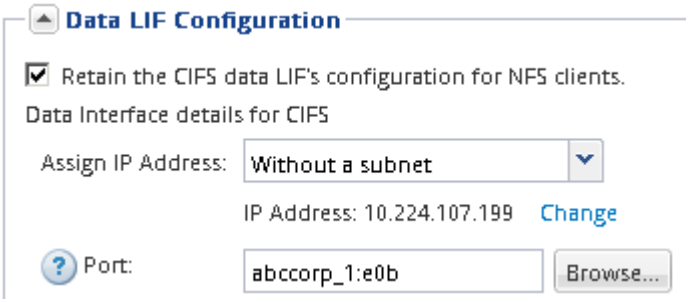
g. 제출 및 계속 * 을 클릭합니다.

SVM이 생성되지만 프로토콜이 아직 구성되지 않았습니다.

4. CIFS/NFS 프로토콜 구성 * 페이지의 * 데이터 LIF 구성 * 섹션에서 클라이언트가 데이터에 액세스하는 데 사용할 LIF의 세부 정보를 지정합니다.

   a. 지정한 서브넷에서 자동으로 LIF에 IP 주소를 할당하거나 수동으로 주소를 입력합니다.

   b. 찾아보기 * 를 클릭하고 LIF와 연결할 노드와 포트를 선택합니다.



5. CIFS 서버 구성 * 섹션에서 CIFS 서버를 정의하고 AD 도메인에 액세스하도록 구성합니다.

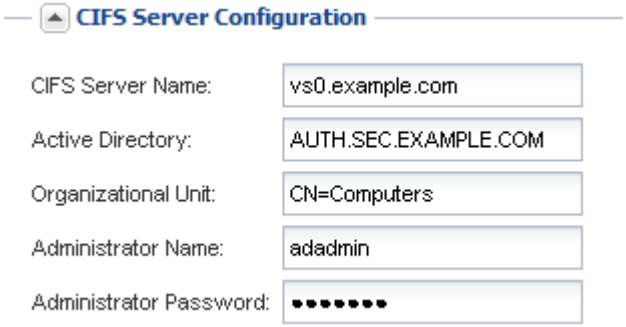
   a. AD 도메인에서 고유한 CIFS 서버의 이름을 지정합니다.

   b. CIFS 서버가 연결할 수 있는 AD 도메인의 FQDN을 지정합니다.

   c. CN=Computers가 아닌 AD 도메인 내의 OU(조직 구성 단위)를 연결하려면 OU를 입력합니다.

   d. OU에 CIFS 서버를 추가할 수 있는 권한이 충분한 관리 계정의 이름과 암호를 지정합니다.

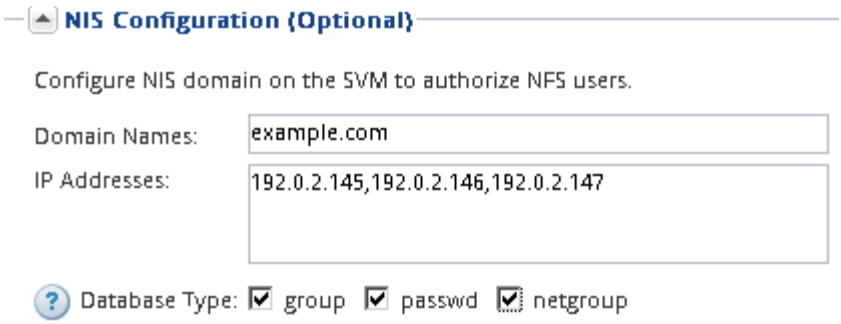
   e. 이 SVM의 모든 공유에 대한 무단 액세스를 방지하려면 SMB 3.0을 사용하여 데이터를 암호화하는 옵션을 선택합니다.



6. CIFS 스토리지 * 영역에 볼륨 용량 할당을 건너뛰십시오. 다중 프로토콜 액세스가 아닌 CIFS 액세스에만 볼륨을 프로비저닝하기 때문입니다.

7. NIS 구성 * 영역이 축소되면 확장합니다.

8. 사이트에서 NIS를 이름 서비스 또는 이름 매핑에 사용하는 경우 NIS 서버의 도메인 및 IP 주소를 지정합니다.



9. NFS 액세스만을 위한 볼륨을 프로비저닝하기 때문에 * NFS 스토리지 * 영역에 볼륨 용량 할당을 건너뜁니다. 멀티 프로토콜 액세스에는 볼륨이 제공되지 않습니다.
10. 제출 및 계속 * 을 클릭합니다.

    다음 오브젝트가 생성됩니다.

    - ""_cifs_nfs_lif1" 접미사를 사용하여 SVM 뒤에 이름이 지정된 데이터 LIF
    - AD 도메인의 일부인 CIFS 서버입니다
    - NFS 서버
11. 표시되는 다른 모든 프로토콜 구성 페이지의 경우 * Skip * (건너뛰기 *)을 클릭하고 나중에 프로토콜을 구성합니다.
12. SVM 관리 * 페이지가 표시되면 이 SVM에 대한 별도의 관리자 구성을 구성하거나 연기합니다.
    - Skip * 을 클릭하고 필요한 경우 나중에 관리자를 구성합니다.
    - 요청된 정보를 입력한 다음 * 제출 및 계속 * 을 클릭합니다.
13. 요약 * 페이지를 검토하고 나중에 필요한 정보를 모두 기록한 다음 * 확인 * 을 클릭합니다.

    DNS 관리자는 CIFS 서버 이름과 데이터 LIF의 IP 주소를 알아야 합니다. Windows 클라이언트는 CIFS 서버의 이름을 알아야 합니다. NFS 클라이언트는 데이터 LIF의 IP 주소를 알아야 합니다.

결과

동일한 데이터 LIF를 통해 CIFS 서버와 NFS 서버에 액세스할 수 있는 새 SVM이 생성됩니다.

다음 단계

이제 SVM 루트 볼륨의 엑스포트 정책을 열어야 합니다.

- 관련 정보 *

SVM 루트 볼륨의 엑스포트 정책 열기(새 NFS 지원 SVM 생성)

기존 **SVM**에 **CIFS** 및 **NFS** 액세스를 추가합니다

기존 SVM에 CIFS/SMB 및 NFS 액세스를 모두 추가하려면 데이터 LIF를 생성하고, CIFS 서버를 구성하고, NFS를 사용하도록 설정하고, 선택적으로 NIS를 구성해야 합니다.

시작하기 전에

- SVM에서 사용할 네트워킹 구성 요소는 무엇입니까?

- 노드 및 해당 노드의 특정 포트에서 데이터 논리 인터페이스(LIF)가 생성됩니다
- 데이터 LIF의 IP 주소를 프로비저닝할 서브넷 또는 선택적으로 데이터 LIF에 할당할 특정 IP 주소를 지정합니다
- SVM을 추가하는 데 필요한 자격 증명과 함께 SVM이 연결할 AD(Active Directory) 도메인입니다
- 사이트에서 NIS를 사용하여 이름 서비스 또는 이름 매핑을 사용하는 경우 NIS 정보입니다

- 모든 외부 방화벽은 네트워크 서비스에 대한 액세스를 허용하도록 적절하게 구성되어야 합니다.
- AD 도메인 컨트롤러, 클라이언트 및 SVM의 시간은 서로 5분 이내에 동기화해야 합니다.
- SVM에서 CIFS 및 NFS 프로토콜을 허용해야 합니다.

  다른 프로토콜을 구성하면서 SVM을 생성하기 위해 이 절차를 따르지 않은 경우에 해당됩니다.

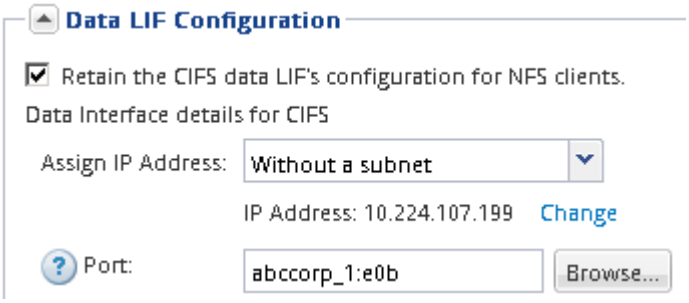
이 작업에 대해

CIFS 및 NFS를 구성하는 순서는 표시되는 대화 상자에 영향을 줍니다. 이 절차에서는 CIFS를 먼저 구성하고 NFS를 다시 구성해야 합니다.

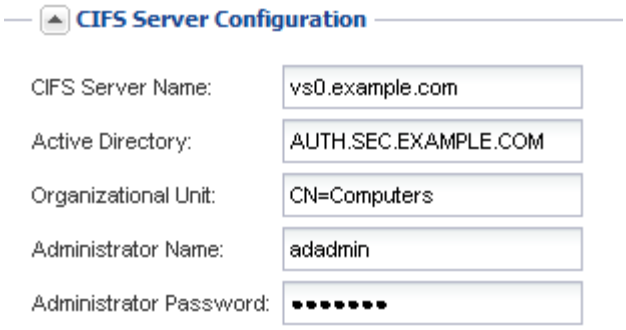
단계

1. SVM의 프로토콜을 구성할 수 있는 영역으로 이동합니다.
   a. 구성할 SVM을 선택합니다.
   b. Details * 창에서 * Protocols * 옆에 있는 * CIFS * 를 클릭합니다.

2. CIFS 프로토콜 구성 * 대화 상자의 * 데이터 LIF 구성 * 섹션에서 SVM용 데이터 LIF를 생성합니다.
   a. 지정한 서브넷에서 자동으로 LIF에 IP 주소를 할당하거나 수동으로 주소를 입력합니다.
   b. 찾아보기 * 를 클릭하고 LIF와 연결할 노드와 포트를 선택합니다.

3. CIFS 서버 구성 * 섹션에서 CIFS 서버를 정의하고 AD 도메인에 액세스하도록 구성합니다.
   a. AD 도메인에서 고유한 CIFS 서버의 이름을 지정합니다.
   b. CIFS 서버가 연결할 수 있는 AD 도메인의 FQDN을 지정합니다.
   c. CN=Computers가 아닌 AD 도메인 내의 OU(조직 구성 단위)를 연결하려면 OU를 입력합니다.
   d. OU에 CIFS 서버를 추가할 수 있는 권한이 충분한 관리 계정의 이름과 암호를 지정합니다.
   e. 이 SVM의 모든 공유에 대한 무단 액세스를 방지하려면 SMB 3.0을 사용하여 데이터를 암호화하는 옵션을 선택합니다.

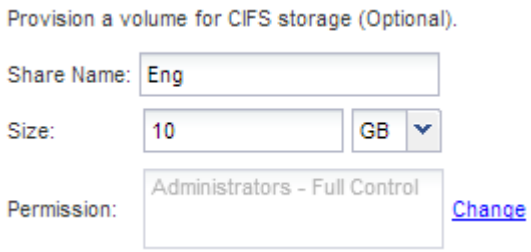


4. CIFS/SMB 액세스를 위한 볼륨을 생성하고 이 볼륨에서 공유를 프로비저닝합니다.

   a. CIFS/SMB 클라이언트가 볼륨을 액세스하는 데 사용할 공유의 이름을 지정합니다.

      공유에 대해 입력한 이름도 볼륨 이름으로 사용됩니다.

   b. 볼륨의 크기를 지정합니다.



   가장 사용 가능한 공간이 있는 애그리게이트에 자동으로 있으므로 볼륨의 애그리게이트를 지정할 필요가 없습니다.

5. CIFS 스토리지 * 영역에 볼륨 용량 할당을 건너뛰십시오. 다중 프로토콜 액세스가 아닌 CIFS 액세스에만 볼륨을 프로비저닝하기 때문입니다.
6. 제출 및 닫기 * 를 클릭한 다음 * 확인 * 을 클릭합니다.
7. NFS 활성화:

   a. SVM 탭에서 NFS를 활성화할 SVM을 선택하고 * 관리 * 를 클릭합니다.

   b. 프로토콜 * 창에서 * NFS * 를 클릭한 다음 * 활성화 * 를 클릭합니다.

8. 사이트에서 NIS를 사용하여 이름 서비스 또는 이름 매핑을 사용하는 경우 NIS를 구성합니다.

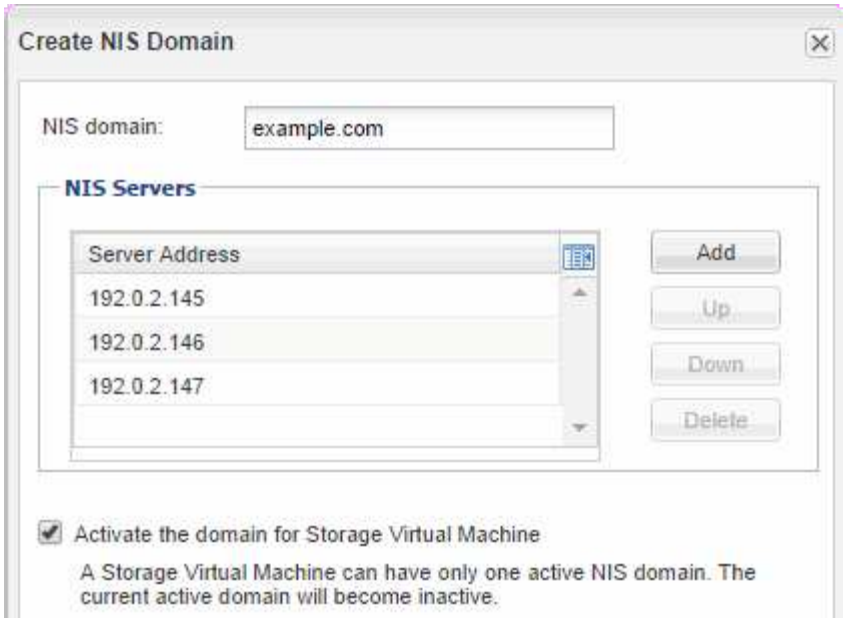
   a. 서비스 * 창에서 * NIS * 를 클릭합니다.

   b. NIS * 창에서 * 생성 * 을 클릭합니다.

   c. NIS 서버의 도메인을 지정합니다.

   d. NIS 서버의 IP 주소를 추가합니다.

   e. 스토리지 가상 머신 * 에 대해 도메인 활성화 를 선택한 다음 * 생성 * 을 클릭합니다.



다음 단계

SVM 루트 볼륨의 엑스포트 정책을 엽니다.

SVM 루트 볼륨의 엑스포트 정책을 엽니다(새 NFS 지원 SVM 생성).

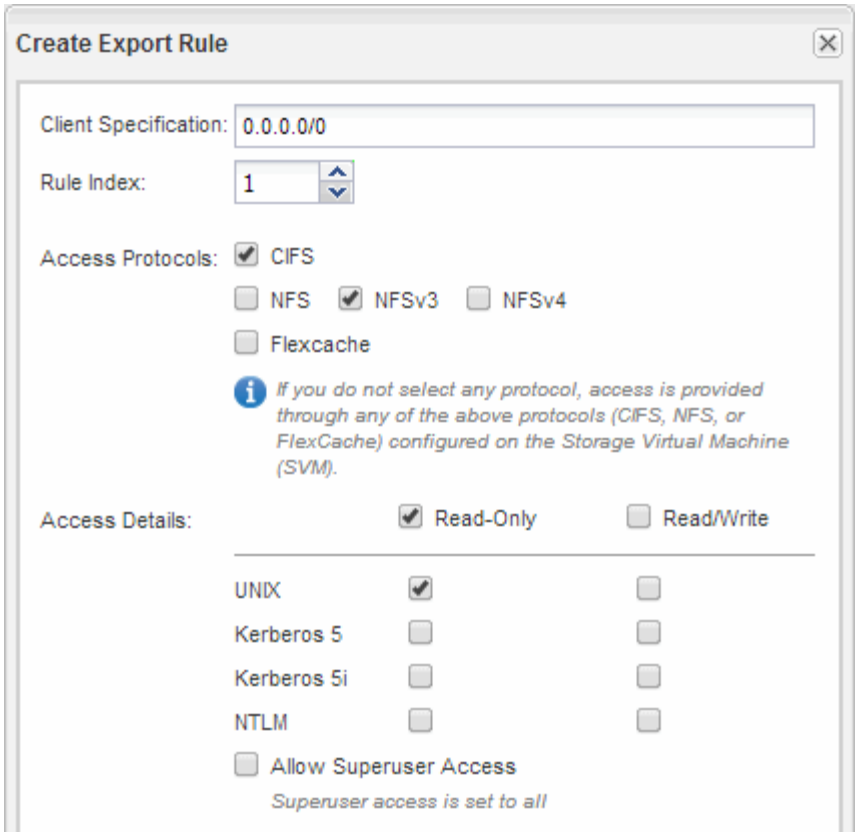
NFSv3을 통해 모든 클라이언트가 액세스할 수 있도록 기본 엑스포트 정책에 규칙을 추가해야 합니다. 이 규칙이 없으면 모든 NFS 클라이언트가 SVM(스토리지 가상 머신) 및 볼륨에 액세스할 수 없습니다.

이 작업에 대해

모든 NFS 액세스를 기본 엑스포트 정책으로 지정하고 나중에 개별 볼륨에 대한 사용자 지정 엑스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. SVM * 창으로 이동합니다.
2. SVM 설정 * 탭을 클릭합니다.
3. Policies * 창에서 * Export Policies * 를 클릭합니다.
4. SVM 루트 볼륨에 적용되는 * default * 라는 엑스포트 정책을 선택합니다.
5. 아래 창에서 * 추가 * 를 클릭합니다.
6. 내보내기 규칙 생성 * 대화 상자에서 NFS 클라이언트의 모든 클라이언트에 대한 액세스를 여는 규칙을 생성합니다.
   a. Client Specification * 필드에 모든 클라이언트에 규칙이 적용되도록 0.0.0.0/0"을 입력합니다.
   b. 규칙 인덱스의 경우 기본값을 * 1 * 로 유지합니다.
   c. NFSv3 * 을 선택합니다.
   d. 읽기 전용 * 아래의 * UNIX * 확인란을 제외한 모든 확인란의 선택을 취소합니다.
   e. 확인 * 을 클릭합니다.



결과

이제 NFSv3 클라이언트가 SVM에서 생성된 모든 볼륨에 액세스할 수 있습니다.

DNS 서버의 SMB 서버를 매핑합니다

Windows 사용자가 SMB 서버 이름에 드라이브를 매핑할 수 있도록 사이트의 DNS 서버에는 SMB 서버 이름 및 모든 NetBIOS 별칭을 가리키는 항목이 데이터 LIF의 IP 주소에 있어야 합니다.

시작하기 전에

사이트의 DNS 서버에 대한 관리 액세스 권한이 있어야 합니다. 관리 액세스 권한이 없는 경우 DNS 관리자에게 이 작업을 수행하도록 요청해야 합니다.

이 작업에 대해

SMB 서버 이름에 NetBIOS 별칭을 사용하는 경우 각 별칭에 대해 DNS 서버 진입점을 만드는 것이 좋습니다.

단계

1. DNS 서버에 로그인합니다.
2. 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 LIF의 IP 주소에 매핑합니다.
3. NetBIOS 별칭을 사용하는 경우 별칭 정규 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버 데이터 LIF의 IP 주소에 매핑합니다.

결과

매핑이 네트워크를 통해 전파되면 Windows 사용자는 드라이브를 SMB 서버 이름 또는 NetBIOS 별칭에 매핑할 수 있습니다.

LDAP 구성(새 NFS 지원 SVM 생성)

SVM(스토리지 가상 시스템)에서 Active Directory 기반 LDAP(Lightweight Directory Access Protocol)의 사용자 정보를 가져오려면 LDAP 클라이언트를 생성하고 SVM용으로 설정한 다음 다른 사용자 정보 소스보다 LDAP 우선 순위를 지정해야 합니다.

시작하기 전에

- LDAP 구성은 AD(Active Directory)를 사용해야 합니다.

  다른 유형의 LDAP를 사용하는 경우 LDAP를 구성하려면 CLI(Command-Line Interface) 및 기타 설명서를 사용해야 합니다.

  "NetApp 기술 보고서 4067: NetApp ONTAP의 NFS"

  "NetApp 기술 보고서 4616: ONTAP에서 Microsoft Active Directory와 NFS Kerberos"

  "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"

- AD 도메인 및 서버는 물론 인증 레벨, Bind 사용자 및 암호, 기본 DN 및 LDAP 포트와 같은 바인딩 정보를 알아야 합니다.

단계

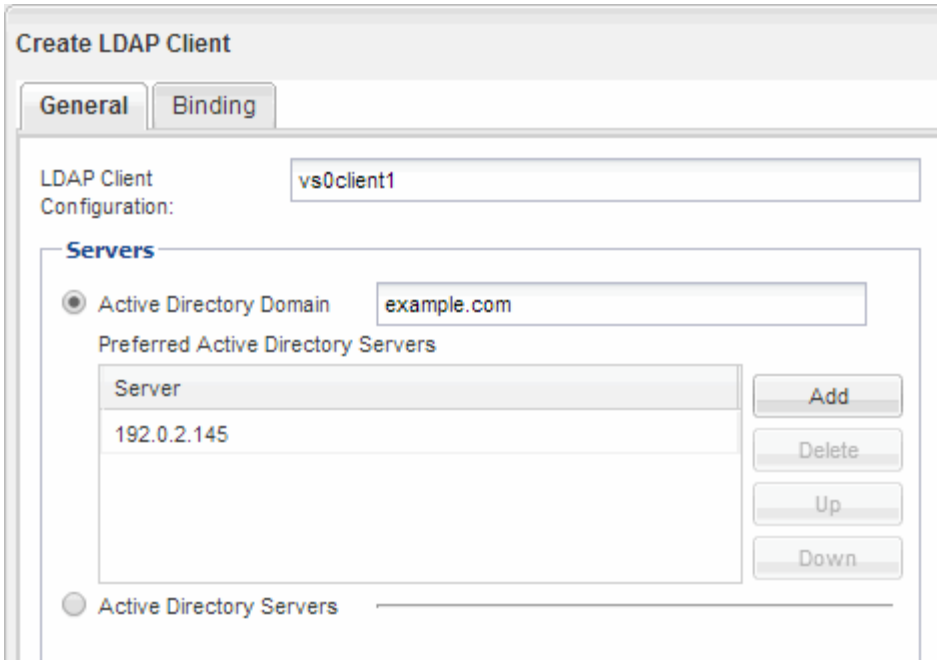
1. SVM * 창으로 이동합니다.
2. 필요한 SVM을 선택합니다
3. SVM 설정 * 탭을 클릭합니다.
4. SVM에서 사용할 LDAP 클라이언트 설정:

   a. 서비스 * 창에서 * LDAP 클라이언트 * 를 클릭합니다.

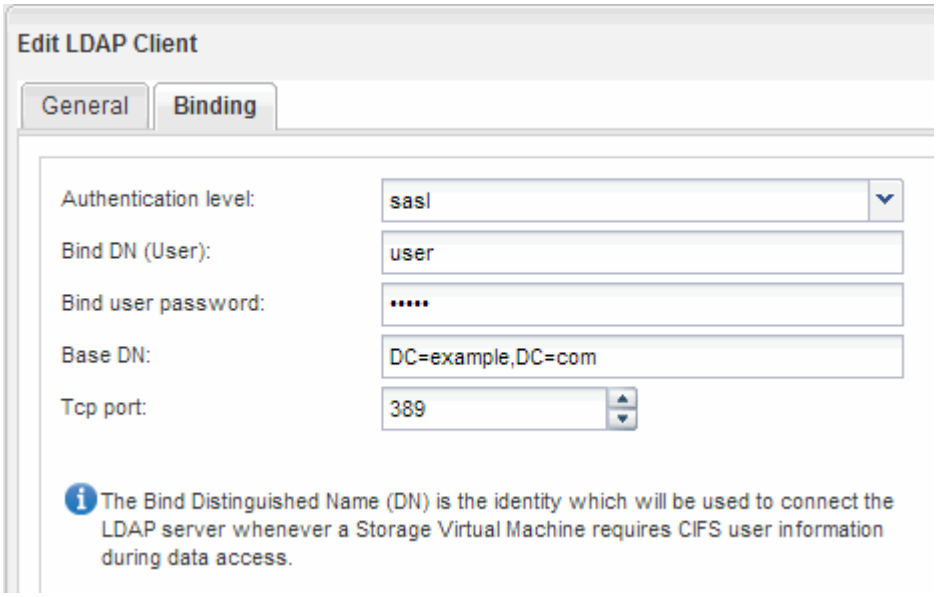
   b. LDAP 클라이언트 구성 * 창에서 * 추가 * 를 클릭합니다.

   c. Create LDAP Client * 창의 * General * 탭에서 "vs0client1"과 같은 LDAP 클라이언트 구성의 이름을 입력합니다.

   d. AD 도메인 또는 AD 서버를 추가합니다.



e. Binding * 을 클릭하고 인증 수준, Bind 사용자 및 암호, 기본 DN 및 포트를 지정합니다.



f. 저장 후 닫기 * 를 클릭합니다.

SVM에서 사용할 수 있도록 새 클라이언트가 생성되고 제공됩니다.

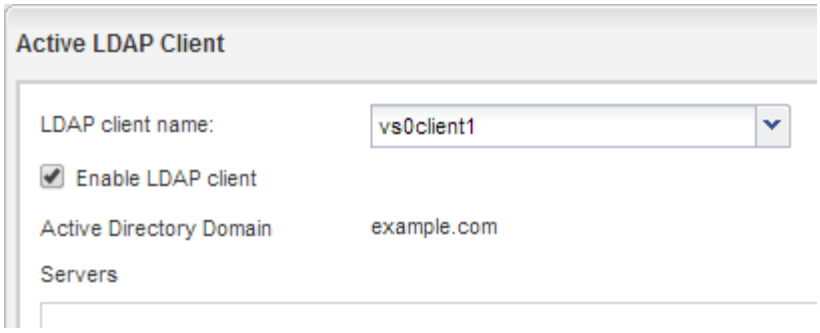
5. SVM을 위한 새 LDAP 클라이언트 지원:

a. 탐색 창에서 * LDAP Configuration * 을 클릭합니다.

b. 편집 * 을 클릭합니다.

c. 방금 생성한 클라이언트가 * LDAP 클라이언트 이름 * 에서 선택되었는지 확인합니다.

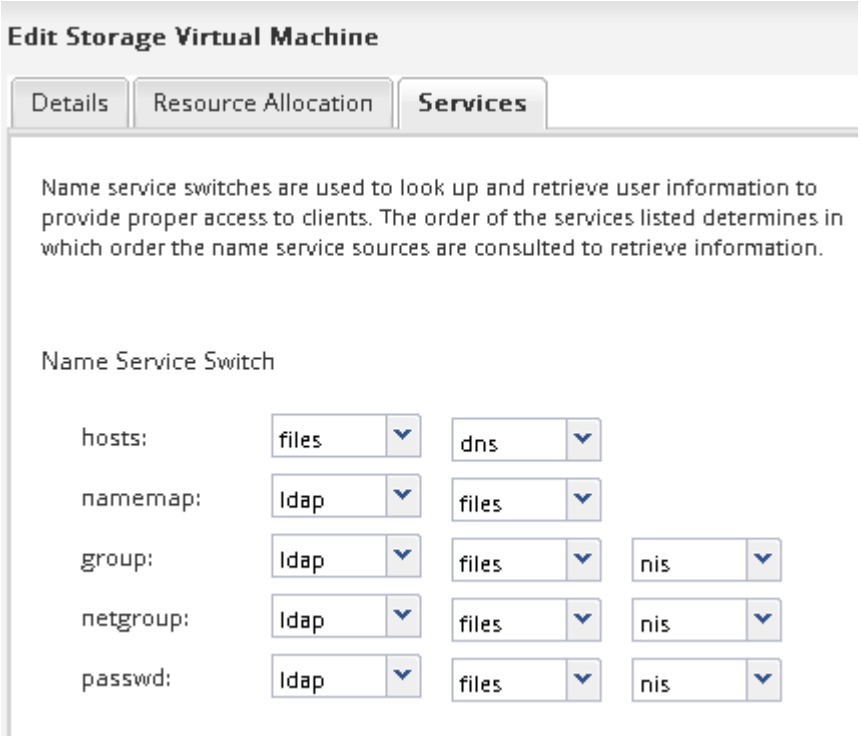
d. LDAP 클라이언트 활성화 * 를 선택하고 * 확인 * 을 클릭합니다.



SVM은 새 LDAP 클라이언트를 사용합니다.

6. NIS(Network Information Service), 로컬 사용자 및 그룹과 같은 다른 사용자 정보 소스보다 LDAP 우선 순위를 지정합니다.

   a. SVM * 창으로 이동합니다.
   b. SVM을 선택하고 * Edit * 를 클릭합니다.
   c. 서비스 * 탭을 클릭합니다.
   d. 이름 서비스 스위치 * 에서 * LDAP * 를 데이터베이스 유형의 기본 이름 서비스 스위치 소스로 지정합니다.
   e. 저장 후 닫기 * 를 클릭합니다.



LDAP는 이 SVM에서 이름 서비스와 이름 매핑을 위한 기본 사용자 정보입니다.

UNIX 및 Windows 사용자 이름을 매핑합니다

사이트에 Windows 및 UNIX 사용자 계정이 모두 있는 경우 이름 매핑을 사용하여 Windows 사용자가 UNIX 파일 권한으로 파일에 액세스하고 UNIX 사용자가 NTFS 파일 권한이 있는

파일에 액세스할 수 있도록 해야 합니다. 이름 매핑에는 암시적 매핑, 변환 규칙 및 기본 사용자의 모든 조합이 포함될 수 있습니다.

이 작업에 대해

이 절차는 사이트에 암시적으로 매핑되지 않는 Windows 및 UNIX 사용자 계정이 있는 경우에만 사용해야 합니다. 즉, 각 Windows 사용자 이름의 소문자 버전이 UNIX 사용자 이름과 일치하는 경우입니다. 이 작업은 NIS, LDAP 또는 로컬 사용자를 사용하여 수행할 수 있습니다. 일치하지 않는 두 사용자 세트가 있는 경우 이름 매핑을 구성해야 합니다.

단계

1. 다음 요소를 고려하여 이름 매핑 방법(이름 매핑 변환 규칙, 기본 사용자 매핑 또는 둘 다)을 결정합니다.
   - 변환 규칙 정규식을 사용하여 한 사용자 이름을 다른 사용자 이름으로 변환합니다. 이 방법은 개별 수준에서 액세스를 제어하거나 추적하려는 경우에 유용합니다.

     예를 들어 UNIX 사용자를 도메인의 Windows 사용자에게 매핑하거나 그 반대로 매핑할 수 있습니다.

   - 기본 사용자는 암시적 매핑이나 이름 매핑 변환 규칙에 의해 매핑되지 않은 모든 사용자에게 사용자 이름을 할당할 수 있습니다.

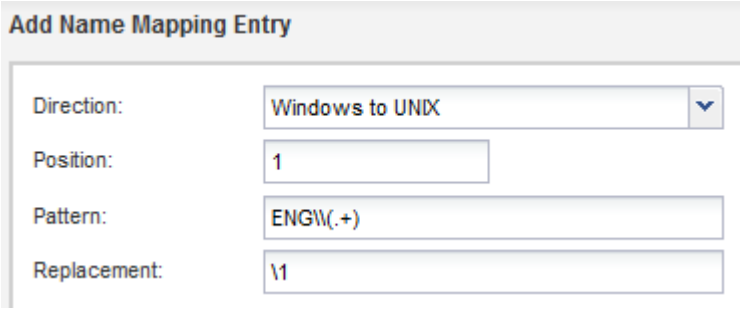
     각 SVM에는 ""pcuser"라는 기본 UNIX 사용자가 있지만 기본 Windows 사용자는 없습니다.

2. SVM * 창으로 이동합니다.
3. 구성할 SVM을 선택합니다.
4. SVM 설정 * 탭을 클릭합니다.
5. * 선택 사항 *: UNIX 사용자 계정을 Windows 사용자 계정으로 변환하는 이름 매핑을 생성합니다. 그 반대의 경우도 마찬가지입니다.

   a. 호스트 사용자 및 그룹 * 창에서 * 이름 매핑 * 을 클릭합니다.

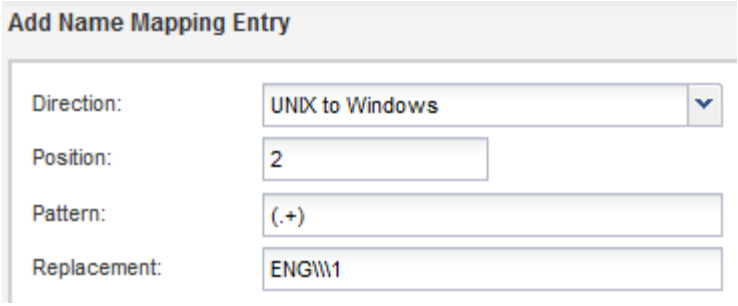
   b. 추가 * 를 클릭하고 기본 * Windows to UNIX * 방향을 유지한 다음 Windows 사용자가 UNIX 파일 권한을 사용하는 파일에 액세스하려고 할 때 UNIX 자격 증명을 생성하는 정규식을 만듭니다.

      다음 항목을 사용하여 ENG 도메인의 모든 Windows 사용자를 같은 이름의 UNIX 사용자로 변환합니다. 패턴 "eng\\\(.+)는 접두사가 "eng\\"인 Windows 사용자 이름을 찾은 다음, 교체 "\1"은 사용자 이름을 제외한 모든 항목을 제거하여 UNIX 버전을 만듭니다.

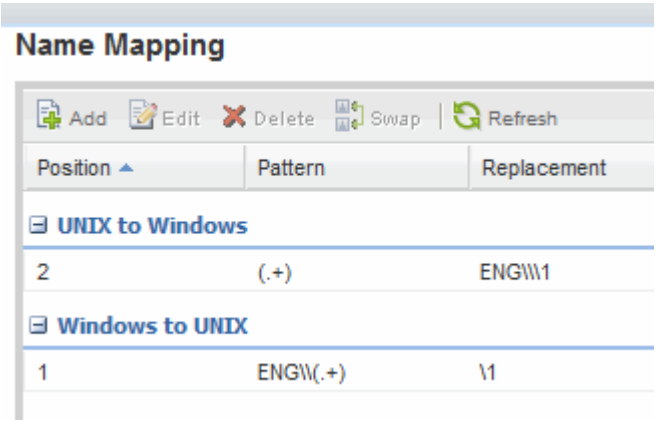
      

   c. 추가** 를 클릭하고 * UNIX to Windows * 방향을 선택한 다음 UNIX 사용자가 NTFS 파일 권한이 있는 파일에 액세스하려고 할 때 Windows 자격 증명을 생성하는 해당 매핑을 만듭니다.

      다음 항목을 사용하여 모든 UNIX 사용자를 ENG 도메인에서 동일한 이름의 Windows 사용자로 변환합니다. 패턴(.+)은 UNIX 이름을 찾은 후 교체 이름이 eng\\\1이면 사용자 이름 앞에 eng\\를 삽입하여 Windows 버전을 만듭니다.



a. 각 규칙의 위치에 따라 규칙이 적용되는 순서가 결정되므로 결과를 검토하고 순서가 사용자의 기대치와 일치하는지 확인해야 합니다.



b. 5b~5d단계를 반복하여 SVM의 모든 도메인과 이름을 매핑합니다.

6. * 선택 사항 *: 기본 Windows 사용자 만들기:

   a. LDAP, NIS 또는 SVM 로컬 사용자에게 Windows 사용자 계정을 생성합니다.

      로컬 사용자를 사용하는 경우 호스트 사용자 및 그룹 창의 * Windows * 에서 계정을 만들 수 있습니다.

   b. 프로토콜 * 창에서 * NFS * > * 편집 * 을 선택하고 사용자 이름을 입력하여 기본 Windows 사용자를 설정합니다.

   ""unixusers""라는 로컬 Windows 사용자를 만들고 이를 기본 Windows 사용자로 설정할 수 있습니다.

7. * 선택 사항*: 사용자가 ""pcuser"" 사용자인 기본값과 다르게 하려면 기본 UNIX 사용자를 구성합니다.

   a. LDAP, NIS 또는 SVM 로컬 사용자에게 UNIX 사용자 계정을 생성합니다.

      로컬 사용자를 사용하는 경우 호스트 사용자 및 그룹 창의 * UNIX * 에서 계정을 만들 수 있습니다.

   b. 프로토콜 * 창에서 * cifs * > * Options * 를 선택하고 사용자 이름을 입력하여 기본 UNIX 사용자를 설정합니다.

   로컬 UNIX 사용자 ""winusers""를 만들어 기본 UNIX 사용자로 설정할 수 있습니다.

다음 단계

기본 사용자를 구성한 경우 나중에 워크플로에서 파일 권한을 구성할 때 기본 Windows 사용자 및 기본 UNIX 사용자에 대한 권한을 설정해야 합니다.

볼륨을 생성하고 구성합니다

데이터를 포함할 FlexVol 볼륨을 만들어야 합니다. 필요에 따라 루트 볼륨의 보안 스타일에서 상속되는 볼륨의 기본 보안 스타일을 변경할 수 있습니다. 스토리지 가상 시스템(SVM)의 루트 볼륨에 있는 네임스페이스에서 볼륨의 기본 위치를 선택적으로 변경할 수도 있습니다.

단계

1. Volumes * 창으로 이동합니다.
2. Create * > * Create FlexVol * 를 클릭합니다.

   Create Volume(볼륨 생성) 대화 상자가 표시됩니다.

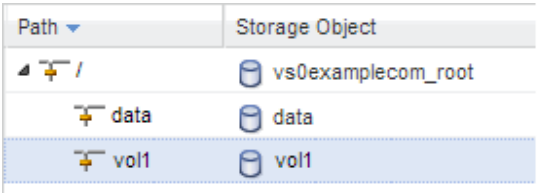
3. 날짜 및 시간 스탬프로 끝나는 기본 이름을 변경하려면 vol1 등의 새 이름을 지정합니다.
4. 볼륨의 애그리게이트를 선택합니다.
5. 볼륨의 크기를 지정합니다.
6. Create * 를 클릭합니다.

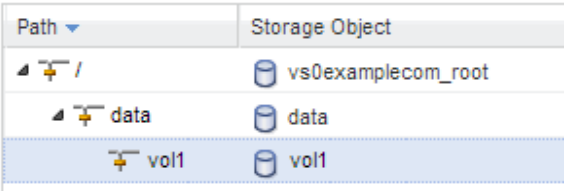
   System Manager에서 생성된 모든 새 볼륨은 기본적으로 루트 볼륨에 접합 이름으로 볼륨 이름을 사용하여 마운트됩니다. CIFS 공유를 구성할 때 접합 경로 및 접합 이름을 사용하고, NFS 클라이언트는 볼륨을 마운트할 때 접합 경로 및 접합 이름을 사용합니다.

7. * 선택 사항 *: SVM의 루트에 볼륨이 위치하지 않도록 하려면 기존 네임스페이스에서 새 볼륨의 위치를 수정합니다.

   a. Namespace* 창으로 이동합니다.
   b. 드롭다운 메뉴에서 * SVM * 을 선택합니다.
   c. Mount * 를 클릭합니다.
   d. 볼륨 마운트 * 대화 상자에서 볼륨, 접합 경로의 이름 및 볼륨을 마운트할 접합 경로를 지정합니다.
   e. Namespace* 창에서 새 접합 경로를 확인합니다.

      "데이터"라는 기본 볼륨 아래에 특정 볼륨을 구성하려면 루트 볼륨에서 "데이터" 볼륨으로 새 볼륨 "vol1"을 이동할 수 있습니다.



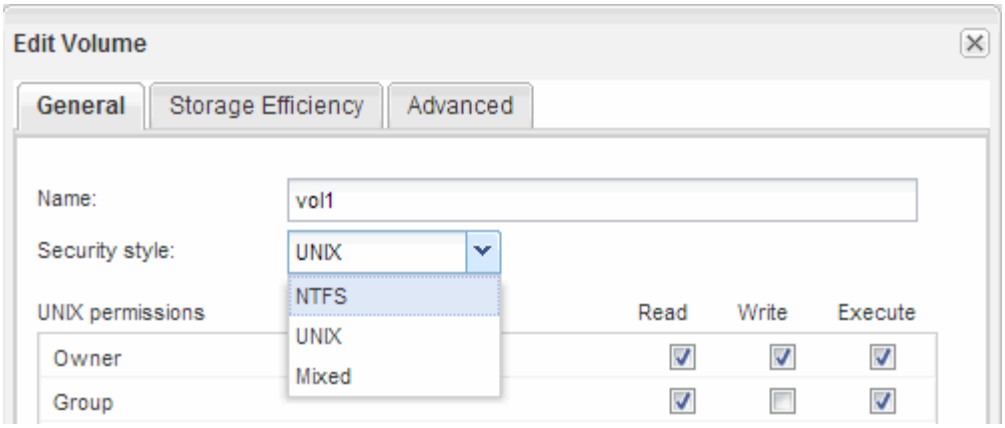


8. 볼륨의 보안 스타일을 검토하고 필요한 경우 변경합니다.

   a. 볼륨 * 창에서 방금 만든 볼륨을 선택하고 * 편집 * 을 클릭합니다.

      볼륨 편집 대화 상자가 표시되며 SVM 루트 볼륨의 보안 스타일에서 상속된 볼륨의 현재 보안 스타일을 보여줍니다.

   b. 원하는 보안 스타일을 선택하고 * 저장 후 닫기 * 를 클릭합니다.



공유를 생성하고 해당 권한을 설정합니다

Windows 사용자가 볼륨에 액세스하려면 먼저 볼륨에 CIFS 공유를 생성하고 공유에 대한 ACL(액세스 제어 목록)을 수정하여 공유에 대한 액세스를 제한해야 합니다.

이 작업에 대해

테스트를 위해 관리자에게만 액세스를 허용해야 합니다. 나중에 볼륨에 액세스할 수 있는지 확인한 후 더 많은 클라이언트에 대한 액세스를 허용할 수 있습니다.

단계

1. Shares * 창으로 이동합니다.
2. SMB 클라이언트가 볼륨에 액세스할 수 있도록 공유를 생성합니다.
   a. 공유 생성 * 을 클릭합니다.
   b. 공유 생성 * 대화 상자에서 * 찾아보기 * 를 클릭하고 네임스페이스 계층 구조를 확장한 다음 이전에 만든 볼륨을 선택합니다.
   c. 공유 이름을 볼륨 이름과 다르게 하려면 공유 이름을 변경합니다.
   d. Create * 를 클릭합니다.

   공유는 Everyone 그룹에 대해 Full Control로 설정된 기본 ACL로 생성됩니다.
3. 공유 ACL을 수정하여 공유에 대한 액세스를 제한합니다.
   a. 공유를 선택한 다음 * 편집 * 을 클릭합니다.
   b. 사용 권한 * 탭에서 * 모든 사용자 * 그룹을 선택한 다음 * 제거 * 를 클릭합니다.
   c. 추가 * 를 클릭한 다음 SVM이 포함된 Windows Active Directory 도메인에 정의된 관리자 그룹의 이름을 입력합니다.
   d. 새 관리자 그룹을 선택한 상태에서 해당 그룹에 대한 모든 권한을 선택합니다.
   e. 저장 후 닫기 * 를 클릭합니다.

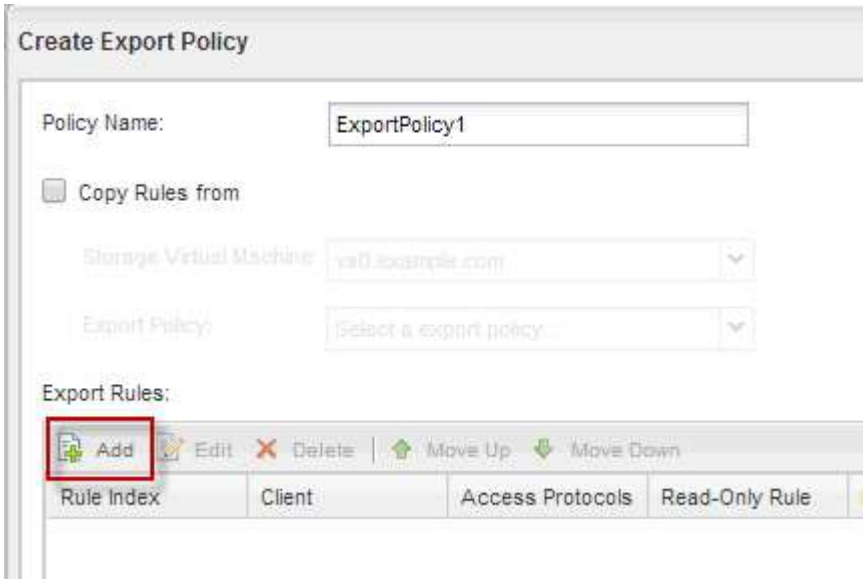
   업데이트된 공유 액세스 권한은 공유 액세스 제어 창에 나열됩니다.

볼륨에 대한 엑스포트 정책을 생성합니다

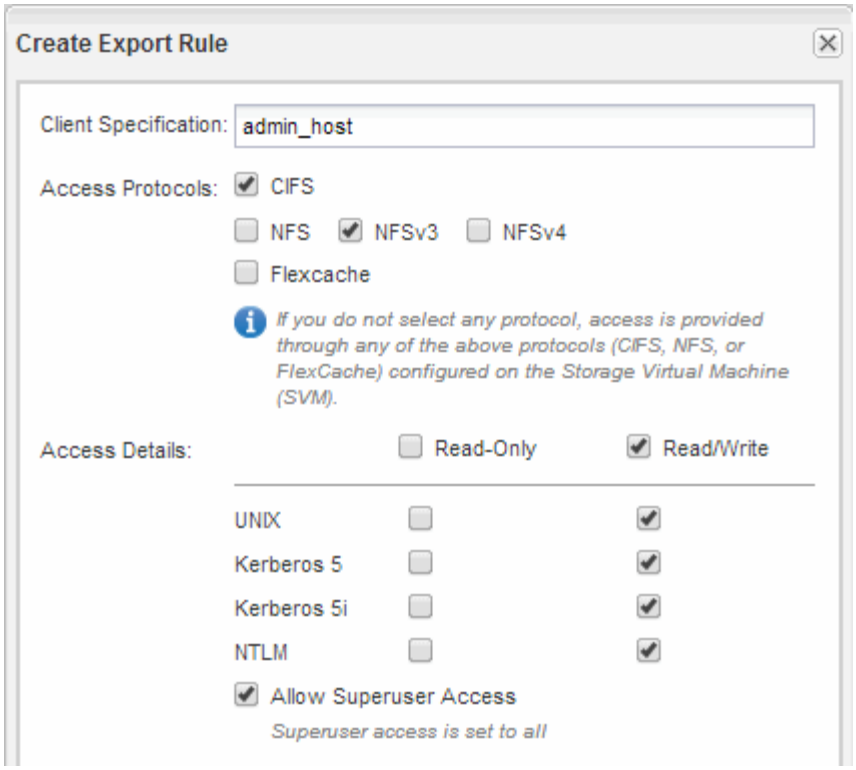
NFS 클라이언트가 볼륨에 액세스하려면 먼저 볼륨에 대한 엑스포트 정책을 생성하고 관리 호스트의 액세스를 허용하는 규칙을 추가한 다음 새 엑스포트 정책을 볼륨에 적용해야 합니다.

단계

1. SVM * 창으로 이동합니다.
2. SVM 설정 * 탭을 클릭합니다.
3. 새 엑스포트 정책 생성:
   a. Policies * 창에서 * Export Policies * 를 클릭한 다음 * Create * 를 클릭합니다.
   b. Create Export Policy * 창에서 정책 이름을 지정합니다.
   c. 내보내기 규칙 * 에서 * 추가 * 를 클릭하여 새 정책에 규칙을 추가합니다.



4. 내보내기 규칙 만들기 * 대화 상자에서 관리자가 모든 프로토콜을 통해 내보내기에 완전히 액세스할 수 있도록 하는 규칙을 만듭니다.
   a. 내보낸 볼륨을 관리할 IP 주소 또는 클라이언트 이름(예: admin_host)을 지정합니다.
   b. CIFS * 및 * NFSv3 * 을 선택합니다.
   c. 모든 * 읽기/쓰기 * 액세스 세부 정보와 * 고급 사용자 액세스 허용 * 이 선택되어 있는지 확인합니다.



d. OK * 를 클릭한 다음 * Create * 를 클릭합니다.

새 엑스포트 정책과 새 규칙이 함께 생성됩니다.

5. 새 볼륨에 새 내보내기 정책을 적용하여 관리자 호스트가 볼륨에 액세스할 수 있도록 합니다.
   a. Namespace* 창으로 이동합니다.
   b. 볼륨을 선택하고 * 내보내기 정책 변경 * 을 클릭합니다.
   c. 새 정책을 선택하고 * 변경 * 을 클릭합니다.

SMB 클라이언트 액세스를 확인합니다

공유에 데이터를 액세스 및 기록하여 SMB를 올바르게 구성했는지 확인해야 합니다. SMB 서버 이름 및 NetBIOS 별칭을 사용하여 액세스를 테스트해야 합니다.

단계

1. Windows 클라이언트에 로그인합니다.
2. SMB 서버 이름을 사용하여 액세스 테스트:
   a. Windows 탐색기에서 드라이브를 공유 위치에 '\s.\\smb_Server_Name\Share_Name' 형식으로 매핑합니다

      매핑에 성공하지 못한 경우 DNS 매핑이 아직 네트워크 전체에 전파되지 않았을 수 있습니다. 나중에 SMB 서버 이름을 사용하여 액세스를 테스트해야 합니다.

      SMB 서버의 이름이 vs1.example.com 이고 공유 이름이 share1 인 경우 '\n.\vs0.example.com\SHARE1` 을 입력해야 합니다

   b. 새로 만든 드라이브에서 테스트 파일을 만든 다음 파일을 삭제합니다.

SMB 서버 이름을 사용하여 공유에 대한 쓰기 액세스를 확인했습니다.

3. NetBIOS 별칭에 대해 2단계를 반복합니다.

UNIX 관리 호스트에서 NFS 액세스를 확인합니다

SVM(Storage Virtual Machine)에 대한 NFS 액세스를 구성한 후에는 NFS 관리 호스트에 로그인하고 SVM에서 데이터를 읽고 쓰는 방법으로 구성을 확인해야 합니다.

시작하기 전에

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

단계

1. 클라이언트 시스템에 루트 사용자로 로그인합니다.
2. cd /mnt/'를 입력하여 디렉토리를 마운트 폴더로 변경합니다.
3. SVM의 IP 주소를 사용하여 새 폴더를 생성하고 마운트합니다.

   a. mkdir /mnt/folder를 입력하여 새 폴더를 만듭니다.

   b. 이 새 디렉토리에 볼륨을 마운트하려면 mount -t nfs -o nfsvers=3, hard IPAddress:/volume_name/mnt/folder"를 입력합니다.

   c. cd folder를 입력하여 디렉토리를 새 폴더로 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 nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. 새 파일을 만들고 파일이 있는지 확인한 후 다음 파일에 텍스트를 씁니다.

   a. 테스트 파일을 생성하려면 터치 파일 이름을 입력하십시오.

   b. ls -l filename을 입력하여 파일이 있는지 확인합니다.

   c. cat>filename을 입력하고 텍스트를 입력한 다음 Ctrl+D를 눌러 테스트 파일에 텍스트를 씁니다.

   d. 테스트 파일의 내용을 표시하려면 cat filename을 입력합니다.

   e. rm 파일 이름을 입력하여 테스트 파일을 제거합니다.

   f. CD..를 입력하여 상위 디렉토리로 돌아갑니다.

```
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 ..
```

결과

SVM에 대한 NFS 액세스를 설정했음을 확인했습니다.

CIFS 및 NFS 클라이언트 액세스를 구성하고 확인합니다

준비가 되면 UNIX 또는 NTFS 파일 권한을 설정하고, 공유 ACL을 수정하고, 내보내기 규칙을 추가하여 클라이언트 액세스를 구성할 수 있습니다. 그런 다음 영향을 받는 사용자 또는 그룹이 볼륨에 액세스할 수 있는지 테스트해야 합니다.

단계

1. 공유에 액세스할 수 있는 클라이언트 및 사용자 또는 그룹을 결정합니다.
2. 볼륨의 보안 스타일에 해당하는 방법을 사용하여 파일 권한을 설정합니다.

볼륨의 보안 스타일이 다음과 같은 경우...	수행할 작업...
NTFS입니다	a. NTFS 권한을 관리할 수 있는 충분한 관리 권한이 있는 관리자로 Windows 클라이언트에 로그인합니다. b. Windows 탐색기에서 드라이브를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * 을 선택합니다. c. 보안 탭을 선택하고 필요에 따라 그룹 및 사용자에 대한 보안 설정을 조정합니다.
Unix	UNIX 관리 호스트에서 루트 사용자를 사용하여 볼륨에 대한 UNIX 소유권 및 권한을 설정합니다.

3. System Manager에서 공유 ACL을 수정하여 Windows 사용자 또는 그룹이 공유에 액세스할 수 있도록 합니다.
   a. Shares * 창으로 이동합니다.
   b. 공유를 선택하고 * 편집 * 을 클릭합니다.
   c. 사용 권한 * 탭을 선택하고 사용자 또는 그룹에 공유에 대한 액세스 권한을 부여합니다.
4. System Manager에서 내보내기 정책에 규칙을 추가하여 NFS 클라이언트가 공유에 액세스하도록 허용합니다.

a. SVM(스토리지 가상 시스템)을 선택하고 * SVM 설정 * 을 클릭합니다.

b. Policies * 창에서 * Export Policies * 를 클릭합니다.

c. 볼륨에 적용되는 엑스포트 정책을 선택합니다.

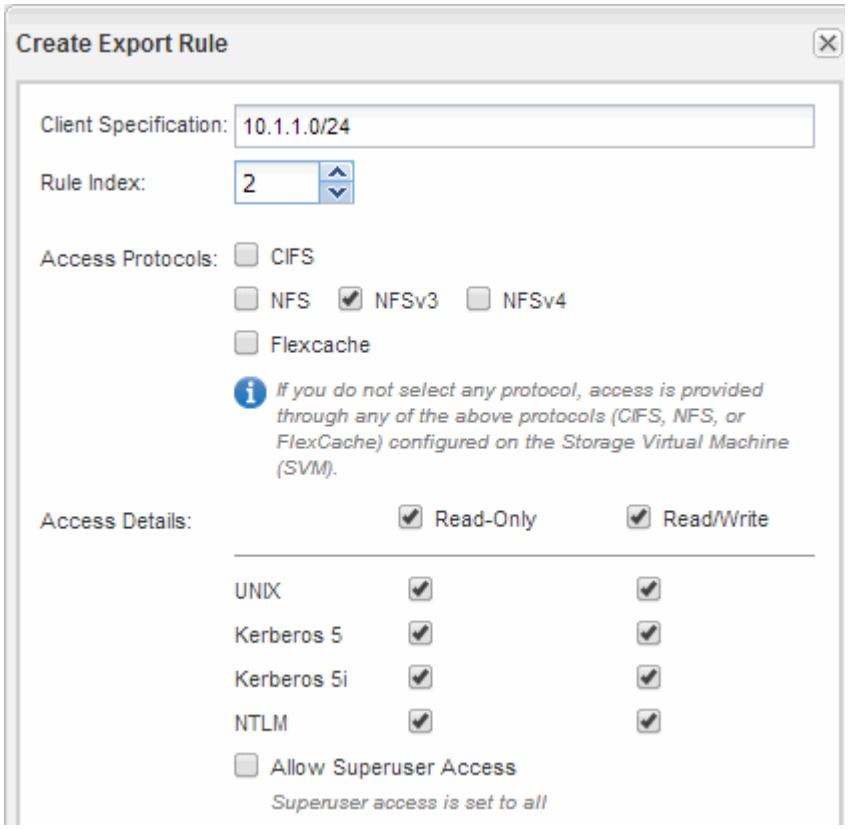
d. 내보내기 규칙 * 탭에서 * 추가 * 를 클릭하고 클라이언트 집합을 지정합니다.

e. 규칙 인덱스 * 에 대해 * 2 * 를 선택하여 이 규칙이 관리 호스트에 대한 액세스를 허용하는 규칙 이후에 실행되도록 합니다.

f. CIFS * 및 * NFSv3 * 을 선택합니다.

g. 원하는 액세스 세부 정보를 지정하고 * 확인 * 을 클릭합니다

   Client Specification * 로 서브넷 10.1.1.0/24 를 입력하고, 슈퍼유저 액세스 허용 * 을 제외한 모든 액세스 확인란을 선택하여 클라이언트에 대한 전체 읽기/쓰기 권한을 부여할 수 있습니다.



5. Windows 클라이언트에서 이제 공유 및 파일에 액세스할 수 있는 사용자 중 하나로 로그인하고 공유에 액세스하고 파일을 생성할 수 있는지 확인합니다.

6. UNIX 클라이언트에서 이제 볼륨에 액세스할 수 있는 사용자 중 하나로 로그인하여 볼륨을 마운트하고 파일을 생성할 수 있는지 확인합니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.