



# CLI를 사용하여 SMB를 구성합니다

## ONTAP 9

NetApp  
April 24, 2024

# 목차

CLI를 사용하여 SMB를 구성합니다 .....	1
CLI를 사용한 SMB 구성 개요 .....	1
SMB 구성 워크플로우 .....	1
준비 .....	2
SVM에 대한 SMB 액세스를 구성합니다 .....	11
공유 스토리지에 대한 SMB 클라이언트 액세스를 구성합니다 .....	32

# CLI를 사용하여 SMB를 구성합니다

## CLI를 사용한 SMB 구성 개요

ONTAP 9 CLI 명령을 사용하여 새 SVM이나 기존 SVM에서 새 볼륨 또는 qtree에 포함된 파일에 대한 SMB 클라이언트 액세스를 구성할 수 있습니다.



*smb*(서버 메시지 블록)는 CIFS(Common Internet File System) 프로토콜의 최신 방언을 의미합니다. ONTAP CLI(Command-Line Interface) 및 OnCommand 관리 툴에서도 *\_cifs\_*가 계속 표시됩니다.

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

- SMB 버전 2 이상을 사용하려고 합니다.
- NFS 클라이언트(멀티 프로토콜 구성 아님)가 아니라 SMB 클라이언트만 지원합니다.
- NTFS 파일 권한은 새 볼륨을 보호하는 데 사용됩니다.
- SVM 관리자 권한이 아닌 클러스터 관리자 권한이 있습니다.

SVM 및 LIF를 생성하려면 클러스터 관리자 권한이 필요합니다. SVM 관리자 권한으로 다른 SMB 구성 작업을 수행할 수 있습니다.

- System Manager나 자동화된 스크립팅 도구가 아니라 CLI를 사용하려고 합니다.

System Manager를 사용하여 NAS 다중 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 CLI 도움말 및 ONTAP man 페이지를 참조하십시오.

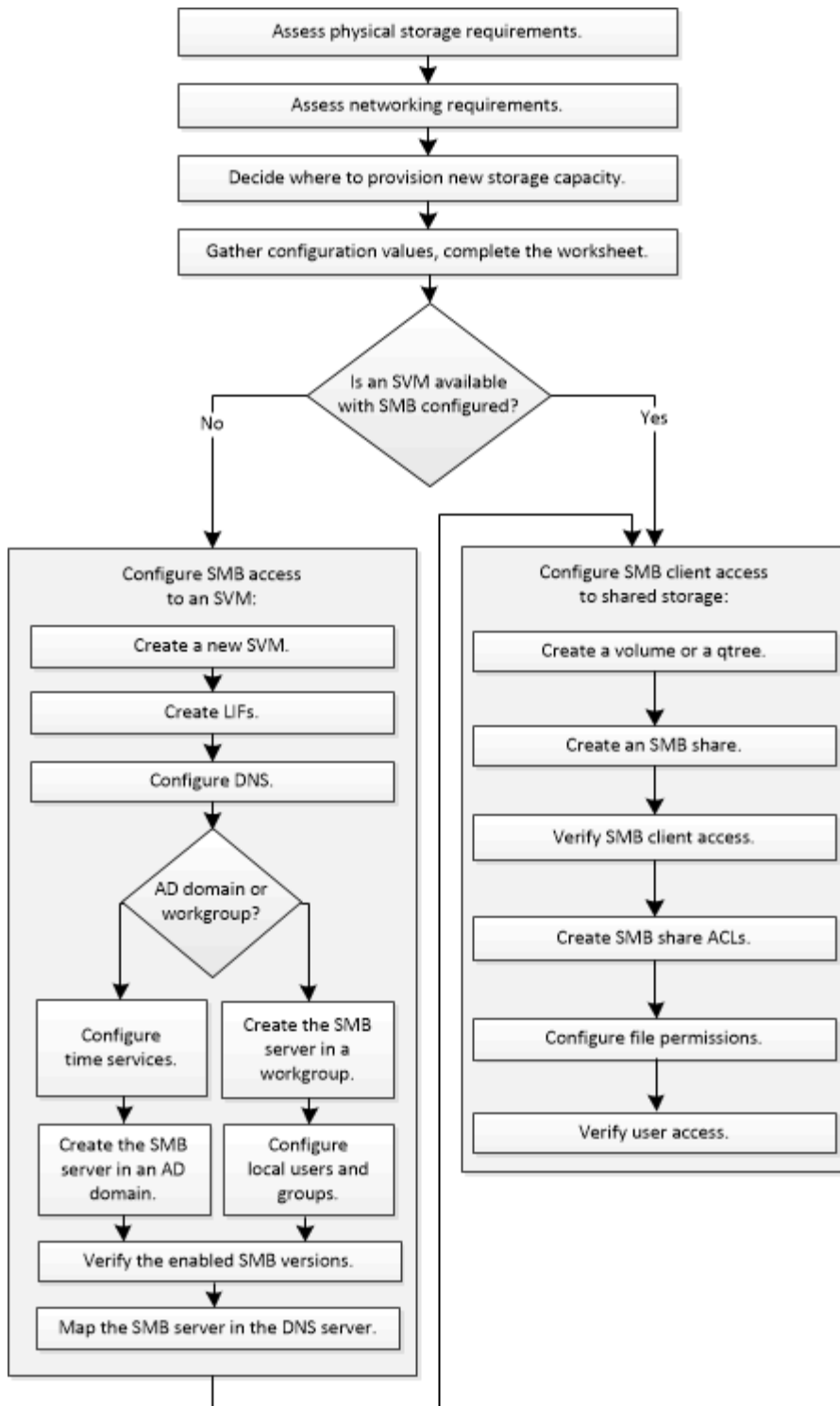
ONTAP SMB 프로토콜 기능 범위에 대한 자세한 내용은 을 참조하십시오 ["SMB 참조 개요"](#).

## ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	자세한 내용은...
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	<a href="#">"SMB를 사용하여 Windows 서버용 NAS 스토리지 용량 할당"</a>
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	<a href="#">"SMB 구성 개요"</a>

## SMB 구성 워크플로우

SMB를 구성하려면 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음 목표에 맞는 워크플로우를 선택하고, 새 SVM 또는 기존 SVM에 SMB 액세스를 구성하거나, SMB 액세스에 대해 이미 완벽하게 구성된 기존 SVM에 볼륨 또는 qtree를 추가해야 합니다.



## 준비

물리적 스토리지 요구사항을 평가합니다

클라이언트용 SMB 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 집계에서 사용 가능한 공간 표시: '스토리지 집계 표시'

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.

## 네트워킹 요구 사항을 평가합니다

SMB 스토리지를 클라이언트에 제공하기 전에 네트워킹이 SMB 프로비저닝 요구 사항을 충족하도록 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 포트와 가상 포트를 네트워크 포트 쇼로 표시합니다

- 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.

◦ 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.

2. 서브넷 이름을 사용하여 LIF에 대한 IP 주소와 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하는지, 사용 가능한 충분한 주소가 있는지 확인하십시오. 'network subnet show'

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

3. 사용 가능한 IPspace 표시: '네트워크 IPspace 쇼'

기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

4. IPv6 주소를 사용하려면 클러스터에서 IPv6가 활성화되어 있는지 확인합니다. 'network options ipv6 show'

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

## 새 **SMB** 스토리지 용량을 프로비저닝할 위치를 결정합니다

새 SMB 볼륨 또는 qtree를 생성하기 전에 새로운 SVM이나 기존 SVM에 배치할 것인지, SVM에 필요한 구성의 양을 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

### 선택

- 새 SVM에서 볼륨 또는 qtree를 프로비저닝하거나 SMB가 활성화되었지만 구성되지 않은 기존 SVM에서 프로비저닝하려는 경우 "'SVM에 SMB 액세스 구성' 및 "'SMB 지원 SVM에 스토리지 용량 추가" 단계를 완료하십시오.

#### SVM에 대한 SMB 액세스 구성

#### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

다음 중 하나에 해당하는 경우 새 SVM을 생성할 수 있습니다.

- 클러스터에서 SMB를 처음으로 활성화하는 경우
- SMB 지원을 사용하지 않으려는 클러스터에 기존 SVM이 있습니다.
- 클러스터에 하나 이상의 SMB 지원 SVM이 있으며 다음 연결 중 하나를 원합니다.
  - 다른 Active Directory 포리스트 또는 워크그룹에.
  - SMB 서버(멀티 테넌시 시나리오) 또한 이 옵션을 선택하여 SMB를 활성화했지만 구성되지 않은 기존 SVM에서 스토리지를 프로비저닝해야 합니다. 이는 SAN 액세스를 위해 SVM을 생성했거나, SVM 생성 시 프로토콜을 사용하지 않은 경우에 발생할 수 있습니다.

SVM에서 SMB를 활성화한 후 볼륨 또는 qtree를 계속해서 프로비저닝합니다.

- SMB 액세스를 위해 완벽하게 구성된 기존 SVM에서 볼륨 또는 qtree를 프로비저닝하려면 "'SMB 지원 SVM에 스토리지 용량 추가" 단계를 완료하십시오.

#### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

## SMB 구성 정보 수집을 위한 워크시트입니다

SMB 구성 워크시트를 사용하면 클라이언트에 대한 SMB 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 SMB 액세스를 구성하는 경우 두 섹션을 모두 완료해야 합니다.

### SVM에 대한 SMB 액세스 구성

#### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

- SMB 지원 SVM에 스토리지 용량을 추가하려면 두 번째 섹션만 완료해야 합니다.

#### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

명령 man 페이지에는 매개 변수에 대한 세부 정보가 포함되어 있습니다.

## SVM에 대한 SMB 액세스 구성

- 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 SMB 스토리지 용량을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-rootvolume'	SVM 루트 볼륨에 제공하는 고유 이름입니다.	
'-rootvolume-security-style'	SVM에 NTFS 보안 스타일을 사용하십시오.	NTFS
'-언어'	이 워크플로의 기본 언어 설정을 사용합니다.	1. UTF-8
'IPSpace'	선택 사항: IPspace는 SVM이 상주하는 별개의 IP 주소 공간입니다.	

- LIF 생성을 위한 매개 변수 \*

LIF를 생성할 때 이러한 값을 'network interface create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-lif'	새 LIF에 대해 제공한 이름입니다.	
'-역할'	이 워크플로우에서 데이터 LIF 역할을 사용합니다.	다타
'-데이터-프로토콜'	이 워크플로우에서는 SMB 프로토콜만 사용합니다.	'CIFS'입니다
홈 노드	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행할 때 LIF가 반환되는 노드입니다.	
``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
자동 되돌리기	선택 사항: 데이터 LIF가 시작 시 또는 다른 상황에서 홈 노드로 자동 전환되는지 여부를 지정합니다. 기본 설정은 false입니다.	

- 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	



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

### Active Directory 도메인에서 SMB 서버 설정

시간 서비스 구성에 대한 매개 변수 \*

시간 서비스를 구성할 때 이러한 값을 'cluster time-service ntp server create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-서버'	Active Directory 도메인에 대한 NTP 서버의 호스트 이름 또는 IP 주소입니다.	

• Active Directory 도메인에서 SMB 서버를 생성하기 위한 매개 변수 \*

새 SMB 서버를 생성하고 도메인 정보를 지정할 때 이러한 값을 'vserver cifs create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 서버를 생성할 SVM의 이름입니다.	
'-cifs-server'	SMB 서버의 이름(최대 15자).	
'도메인'	SMB 서버와 연결할 Active Directory 도메인의 FQDN(정규화된 도메인 이름)입니다.	
'-ou'	선택 사항: SMB 서버와 연결할 Active Directory 도메인 내의 조직 단위입니다. 기본적으로 이 매개 변수는 CN=Computers로 설정됩니다.	
'-NetBIOS-별칭'	선택 사항: NetBIOS 별칭 목록으로, SMB 서버 이름에 대한 대체 이름입니다.	
'논평'	선택 사항: 서버에 대한 텍스트 설명입니다. Windows 클라이언트는 네트워크에서 서버를 검색할 때 이 SMB 서버 설명을 볼 수 있습니다.	

## 작업 그룹에서 **SMB** 서버 설정

- 작업 그룹에서 SMB 서버를 생성하기 위한 매개 변수 \*

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

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 서버를 생성할 SVM의 이름입니다.	
'-cifs-server'	SMB 서버의 이름(최대 15자).	
``워크그룹``	작업 그룹의 이름(최대 15자).	
``논평``	선택 사항: 서버에 대한 텍스트 설명입니다. Windows 클라이언트는 네트워크에서 서버를 검색할 때 이 SMB 서버 설명을 볼 수 있습니다.	

- 로컬 사용자 생성을 위한 매개 변수 \*

'vserver cifs users-and-groups local-user create' 명령을 사용하여 로컬 사용자를 생성할 때 이러한 값을 제공합니다. 이러한 서버는 작업 그룹의 SMB 서버에 필요하며 AD 도메인의 선택적 서버에 필요합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	로컬 사용자를 생성할 SVM의 이름입니다.	
'-user-name'입니다	로컬 사용자의 이름(최대 20자).	
이름	선택 사항: 사용자의 전체 이름입니다. 전체 이름에 공백이 포함된 경우 전체 이름을 큰따옴표로 묶습니다.	
``설명``	선택 사항: 로컬 사용자에 대한 설명입니다. 설명에 공백이 있으면 매개 변수를 따옴표로 묶어야 합니다.	
'-is-account-disabled'	선택 사항: 사용자 계정의 사용 여부를 지정합니다. 이 매개 변수를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다.	

- 로컬 그룹 생성을 위한 매개 변수 \*

'vserver cifs users-and-groups local-group create' 명령을 사용하여 로컬 그룹을 생성할 때 이러한 값을 제공합니다.

AD 도메인 및 워크그룹의 SMB 서버에 대해서는 선택 사항입니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	로컬 그룹을 생성할 SVM의 이름입니다.	
``그룹 이름``	로컬 그룹의 이름입니다(최대 256자).	
``설명``	선택 사항: 로컬 그룹에 대한 설명입니다. 설명에 공백이 있으면 매개 변수를 따옴표로 묶어야 합니다.	

### SMB 지원 SVM에 스토리지 용량 추가

- 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 SMB 볼륨을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-size'	새 볼륨의 크기에 대해 제공하는 정수입니다.	
'-보안-스타일'	이 워크플로에 NTFS 보안 스타일을 사용합니다.	NTFS
``교차점-경로``	새 볼륨을 마운트할 루트(/) 아래의 위치입니다.	

- 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.	

- SMB 공유 생성을 위한 매개 변수 \*

이러한 값은 'vserver cifs share create' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 공유를 생성할 SVM의 이름입니다.	
'-공유-이름'	생성할 SMB 공유의 이름입니다(최대 256자).	
'-경로'	SMB 공유의 경로 이름(최대 256자). 공유를 생성하기 전에 이 경로가 볼륨에 있어야 합니다.	
'-공유-속성'	선택 사항: 공유 속성 목록입니다. 기본 설정은 oplocks, 탐색 가능, changentify, swing-previous-versions입니다.	
'`논평`'	선택 사항: 서버에 대한 텍스트 설명입니다(최대 256자). Windows 클라이언트는 네트워크에서 탐색할 때 이 SMB 공유 설명을 볼 수 있습니다.	

- SMB ACL(공유 액세스 제어 목록) 생성을 위한 매개 변수 \*

이러한 값은 'vserver cifs share access-control create' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB ACL을 생성할 SVM의 이름입니다.	
'-share'	생성할 SMB 공유의 이름입니다.	
'-user-group-type'입니다	공유의 ACL에 추가할 사용자 또는 그룹의 유형입니다. 기본 유형은 Windows입니다	"창"
'- 사용자 또는 그룹'	공유의 ACL에 추가할 사용자 또는 그룹입니다. 사용자 이름을 지정하는 경우 "domain\username" 형식을 사용하여 사용자의 도메인을 포함해야 합니다.	
허락	사용자 또는 그룹에 대한 권한을 지정합니다.	'[No_access
Read	Change	Full_Control]'

## SVM에 대한 SMB 액세스를 구성합니다

### SVM에 대한 SMB 액세스를 구성합니다

SMB 클라이언트 액세스를 위해 SVM이 아직 구성되지 않은 경우 새 SVM을 생성 및 구성하거나 기존 SVM을 구성해야 합니다. SMB를 구성하려면 SVM 루트 볼륨 액세스를 열고, SMB 서버를 생성하고, LIF를 생성하고, 호스트 이름 확인을 지원하고, 이름 서비스를 구성하고, 필요한 경우 Kerberos 보안 활성화.

### SVM을 생성합니다

SMB 클라이언트에 데이터 액세스를 제공하기 위해 클러스터에 SVM을 하나 이상 가지고 있지 않은 경우 하나 생성해야 합니다.

시작하기 전에

- ONTAP 9.13.1 부터는 스토리지 VM의 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 을 참조하십시오 [SVM 용량 관리](#).

단계

1. SVM 생성: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipSPACE ipSPACE_name`
  - '-rootvolume-security-style' 옵션에 NTFS 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 필드에는 CIFS가 포함되어야 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 ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -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 익스포트 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: ntfs
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 9.13.1 부터는 SVM의 볼륨에 처리량 플로어 및 최대 한도를 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 [참조하십시오 적응형 정책 그룹 템플릿을 설정합니다.](#)

## SVM에서 SMB 프로토콜이 활성화되어 있는지 확인합니다

SVM에서 SMB를 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. SVM에 대해 현재 활성화 및 비활성화된 프로토콜은 'vserver show -vserver vserver\_name -protocols'(vserver show -vserver vserver vserver\_name -protocol)를 확인하십시오

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

2. 필요한 경우 프로토콜을 활성화 또는 비활성화합니다.

- SMB 프로토콜을 활성화하려면: 'vserver add-protocols-vserver vserver\_name-protocols cifs'
- 프로토콜을 작동 불가능하게 하려면: "vserver remove-protocols-vserver vserver\_name-protocols protocol\_name[,protocol\_name,...]"

3. 활성화된 프로토콜과 비활성화된 프로토콜이 'vserver show -vserver vserver\_name -protocols'(vserver show -vserver vserver\_name -protocol)로 올바르게 업데이트되었는지 확인합니다

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        cifs                               nfs, fcp, iscsi, ndmp
```

다음 명령을 실행하면 VS1 이라는 SVM의 활성화된 프로토콜 목록에 "CIFS"를 추가하여 SMB를 통해 액세스할 수 있습니다.

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

## SVM 루트 볼륨의 익스포트 정책을 엽니다

SVM 루트 볼륨의 기본 익스포트 정책에는 SMB를 통한 모든 클라이언트의 개방형 액세스를 지원하는 규칙이 포함되어야 합니다. 이러한 규칙이 없으면 모든 SMB 클라이언트가 SVM 및 해당 볼륨에 대한 액세스가 거부됩니다.

이 작업에 대해

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

모든 SMB 액세스가 기본 익스포트 정책에서 열려 있는지 확인하고, 나중에 개별 볼륨 또는 qtree에 대한 사용자 지정 익스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. 기존 SVM을 사용하는 경우 기본 루트 볼륨 익스포트 정책('vserver export-policy rule show')을 확인하십시오

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: cifs
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 익스포트 규칙을 생성합니다. 'vserver export-policy rule create-vserver vserver\_name-policyname default-ruleindex 1-protocol cifs-clientmatch 0.0.0.0/0 -rorule any-rwrule any-superuser any'입니다
3. 'vserver export-policy rule show' 명령을 사용하여 규칙 생성을 확인합니다.

결과

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

## LIF를 생성합니다

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

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 'UP' 상태로 구성되어 있어야 합니다.
- 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.

- 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.

- 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).
- 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.

## 단계

### 1. LIF 생성:

```
'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-
node_node_name_-home-port_port_name_{-address_ip_address_-netmask ip_address_-subnet-
name_subnet_name_-}firewall-policy data-auto-revert{true|false}'
```

\* ONTAP 9.5 이하 \*

```
'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-
node_node_name_-home-port_port_name_{-address_name_- 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_-service-policy_service_policy_name_-
home-node_node_name_-home-port_port_name_{-address_netmask_ip_address_
```

```
-subnet_name_subnet_name_-}firewall-policy data-auto-revert_revert_false
```

- 서비스 정책(ONTAP 9.6부터)을 사용하여 LIF를 생성할 때는 '-role' 매개 변수가 필요하지 않습니다.
- 를 클릭합니다 -data-protocol ONTAP 9.6부터 서비스 정책을 사용하여 LIF를 생성할 때 매개 변수가 필요하지 않습니다. ONTAP 9.5 이하 버전을 사용하는 경우 -data-protocol LIF를 생성할 때 매개 변수를 지정해야 하며 나중에 데이터 LIF를 폐기 및 재생성하지 않고 수정할 수 없습니다.
- 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.

- '-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. '네트워크 라우트 생성' man 페이지에는 SVM 내에서 정적 라우트를 생성하는 정보가 포함되어 있습니다.
- '-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.

## 2. LIF가 성공적으로 생성되었는지 확인합니다.

네트워크 인터페이스 쇼

## 3. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

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

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 cifs -home-node node-4 -home-port elc -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 cifs -home-node node-3 -home-port elc -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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
cluster-1					
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1					
true	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
node-2					
true	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
vs1.example.com					
true	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com					
true	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
```

호스트 이름 확인을 위해 **DNS**를 활성화합니다

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

네트워크 관리 가이드 \_에는 SVM에서 동적 DNS를 구성하는 방법에 대한 정보가 포함되어 있습니다.

단계

1. SVM에서 DNS를 활성화합니다. '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
```



ONTAP 9.2부터 'vserver services name-service dns create' 명령은 자동 구성 검증을 수행하고 ONTAP가 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

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

다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

```
vserver services name-service dns show
```

Vserver	State	Domains	Name 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.

ONTAP 9.2부터 vserver services name-service dns check 명령을 사용할 수 있다.

```
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

## Active Directory 도메인에서 SMB 서버를 설정합니다

시간 서비스를 구성합니다

Active Domain 컨트롤러에서 SMB 서버를 생성하기 전에 SMB 서버가 속할 도메인의 도메인 컨트롤러에 대한 클러스터 시간 및 시간이 5분 이내에 일치하는지 확인해야 합니다.

이 작업에 대해

Active Directory 도메인에서 사용하는 시간 동기화를 위해 클러스터 NTP 서비스를 구성해야 합니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 설정할 수 있습니다.

단계

1. cluster time-service NTP server create 명령을 사용하여 시간 서비스를 구성합니다.
  - 대칭 인증 없이 시간 서비스를 구성하려면 'cluster time-service ntp server create-server\_ip\_address' 명령을 입력합니다
  - 대칭적 인증으로 시간 서비스를 구성하려면 'cluster time-service ntp server create-server\_ip\_address-key-id key-id key\_id"cluster time-service ntp server create-server 10.10.10.1"cluster time-service ntp server create-server 10.10.10.10.10.2' 명령을 입력한다
2. cluster time-service ntp server show 명령을 사용하여 시간 서비스가 올바르게 설정되었는지 확인합니다.

클러스터 시간 서비스 NTP 서버가 표시됩니다

Server	Version
10.10.10.1	auto
10.10.10.2	auto

**NTP** 서버에서 대칭 인증을 관리하는 명령입니다

ONTAP 9.5부터 NTP(네트워크 시간 프로토콜) 버전 3이 지원됩니다. NTPv3에는 SHA-1 키를

사용한 대칭 인증이 포함되어 있어 네트워크 보안을 강화합니다.

수행할 작업...	이 명령 사용...
대칭 인증 없이 NTP 서버를 구성합니다	클러스터 시간 서비스 NTP 서버는 서버 서버 서버 서버 이름(server_name)을 만듭니다
대칭 인증을 사용하여 NTP 서버를 구성합니다	클러스터 시간 서비스 NTP 서버는 '-server"server_ip_address"-key-id"key_id"'를 생성합니다
기존 NTP 서버에 대칭 인증 사용 기존 NTP 서버는 필요한 키 ID를 추가하여 인증을 사용하도록 수정할 수 있습니다	클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 서버 이름 키 ID 키 ID
공유 NTP 키를 구성합니다	<div> 클러스터 시간 서비스 NTP 키는 ``id"sshared_key_id"-type'sshared_key_type'-value'sshared_key_value'를 만듭니다 </div> <div>  공유 키는 ID로 참조됩니다. ID, 유형 및 값은 노드와 NTP 서버 모두에서 동일해야 합니다 </div>
알 수 없는 키 ID로 NTP 서버를 구성합니다	클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다
NTP 서버에 키 ID가 구성되지 않은 서버를 구성합니다.	<div> 클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다 </div> <div>  키 ID, 유형 및 값은 NTP 서버에 구성된 키 ID, 유형 및 값과 동일해야 합니다. </div>
대칭 인증을 사용하지 않도록 설정합니다	클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 이름 인증 비활성화

**Active Directory** 도메인에서 **SMB** 서버를 생성합니다

"vserver cifs create" 명령을 사용하여 SVM에 SMB 서버를 생성하고 해당 서버가 속한 AD(Active Directory) 도메인을 지정할 수 있습니다.

시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 SMB 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버와 SMB 서버에 연결할 도메인의 AD 도메인 컨트롤러에 연결할 수 있어야 합니다.

SMB 서버에 연결할 AD 도메인에서 시스템 계정을 만들 수 있는 권한이 있는 모든 사용자는 SVM에 SMB 서버를 생성할 수 있습니다. 여기에는 다른 도메인의 사용자가 포함될 수 있습니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-uri' 매개 변수에 vserver cifs' 명령을 포함하여 포함시키십시오.

이 작업에 대해

Activity Directory 도메인에서 SMB 서버를 생성하는 경우:

- 도메인을 지정할 때는 FQDN(정규화된 도메인 이름)을 사용해야 합니다.
- 기본 설정은 Active Directory CN=Computer 개체에 SMB 서버 컴퓨터 계정을 추가하는 것입니다.
- '-ou' 옵션을 사용하여 SMB 서버를 다른 OU(조직 구성 단위)에 추가하도록 선택할 수 있습니다.
- SMB 서버에 대해 심표로 구분된 하나 이상의 NetBIOS 별칭 목록(최대 200)을 추가하도록 선택할 수도 있습니다.

SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 서버의 이름에 응답하도록 할 때 유용합니다.

'vserver cifs' man 페이지에는 추가 옵션 매개 변수 및 명명 요구 사항이 포함되어 있습니다.



ONTAP 9.1부터 SMB 버전 2.0을 사용하여 DC(도메인 컨트롤러)에 연결할 수 있습니다. 도메인 컨트롤러에서 SMB 1.0을 사용하지 않도록 설정한 경우 이 작업이 필요합니다. ONTAP 9.2부터는 SMB 2.0이 기본적으로 사용하도록 설정됩니다.

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다. ONTAP는 '-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러 통신을 암호화해야 하며 기본값은 false입니다. SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다. .

"SMB 관리" SMB 서버 구성 옵션에 대한 자세한 내용은 에 나와 있습니다.

단계

1. smb 라이선스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

SMB 라이선스는 에 포함되어 있습니다 ["ONTAP 1 을 참조하십시오"](#). ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이선스가 필요하지 않습니다.

2. AD 도메인에서 SMB 서버를 생성합니다.(+ vserver cifs create -vserver vserver\_name -cifs -server smb\_server\_name -domain FQDN [-ou 조직\_unit] [-NetBIOS-별칭 netbios\_name,...] [-keytab -Uri {(ftp | http)://hostname | ip\_address}] [-comment text]+'

도메인에 참가할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

다음 명령을 실행하면 도메인 " example.com`": 에 SMB 서버 "smb\_server01"이 생성됩니다

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
smb_server01 -domain example.com
```

다음 명령을 실행하면 도메인 "mydomain.com" 에 SMB 서버 "smb\_server02"가 생성되고 keytab 파일을 사용하여 ONTAP 관리자를 인증합니다.



```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

이 예제에서 명령 출력은 "sMB\_SERVER01"이라는 SMB 서버가 SVM vs1.example.com 에서 생성되어 "example.com" 도메인에 가입된 것을 보여 줍니다.

```
cluster1::> vserver cifs show -vserver vs1

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. 필요한 경우 도메인 컨트롤러(ONTAP 9.8 이상)와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver svm\_name -encryption -required-for-dc-connection true'

예

다음 명령을 실행하면 "example.com" 도메인의 SVM vs2.example.com 에 "sMB\_server02" 이름의 SMB 서버가 생성됩니다. 컴퓨터 계정은 "OU=ENG,OU=Corp,DC=example,DC=com" 컨테이너에 생성됩니다. SMB 서버에는 NetBIOS 별칭이 할당됩니다.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

다음 명령을 사용하면 다른 도메인의 사용자(이 경우 신뢰할 수 있는 도메인 관리자)가 SVM vs3.example.com 에 "smb\_server03" 이름의 SMB 서버를 생성할 수 있습니다. '-domain' 옵션은 SMB 서버를 생성하려는 홈 도메인(DNS 구성에 지정됨)의 이름을 지정합니다. 사용자 이름 옵션은 신뢰할 수 있는 도메인의 관리자를 지정합니다.

- 홈 도메인: example.com
- 신뢰할 수 있는 도메인: trust.lab.com
- 신뢰할 수 있는 도메인의 사용자 이름: Administrator1

```
cluster1:~> vsync cifs create -vsync vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com
```

```
Password: . . .
```

**SMB** 인증을 위한 **keytab** 파일을 생성합니다

ONTAP 9.7부터 ONTAP는 keytab 파일을 사용하여 AD(Active Directory) 서버에서 SVM 인증을 지원합니다. AD 관리자는 keytab 파일을 생성하여 ONTAP 관리자가 이를 URI(Uniform Resource Identifier)로 사용할 수 있도록 합니다. 이 URI는 'vsync cifs' 명령에 AD 도메인과의 Kerberos 인증이 필요한 경우에 제공됩니다.

AD 관리자는 표준 Windows Server "ktpass" 명령을 사용하여 keytab 파일을 만들 수 있습니다. 이 명령은 인증이 필요한 기본 도메인에서 실행해야 합니다. "ktpass" 명령은 기본 도메인 사용자에게 대해서만 keytab 파일을 생성하는 데 사용할 수 있으며, trusted-domain 사용자를 사용하여 생성된 키는 지원되지 않습니다.

Keytab 파일은 특정 ONTAP 관리자 사용자를 위해 생성됩니다. admin 사용자의 암호가 변경되지 않는 한, 특정 암호화 유형 및 도메인에 대해 생성된 키는 변경되지 않습니다. 따라서 admin 사용자의 암호를 변경할 때마다 새 keytab 파일이 필요합니다.

지원되는 암호화 유형은 다음과 같습니다.

- AES256-SHA1
- DES-CBC-MD5



ONTAP는 DES-CBC-CRC 암호화 유형을 지원하지 않습니다.

- RC4-HMAC

AES256은 가장 높은 암호화 유형으로, ONTAP 시스템에서 활성화된 경우 사용해야 합니다.

keytab 파일은 admin 암호를 지정하거나 임의로 생성된 암호를 사용하여 생성할 수 있습니다. 그러나 언제든지 한 개의 암호 옵션만 사용할 수 있습니다. AD 서버에서는 키 탭 파일 내의 키를 해독하기 위해 관리자 사용자 고유의 개인 키가 필요하기 때문입니다. 특정 관리자에 대한 개인 키를 변경하면 keytab 파일이 무효화됩니다.

워크그룹에서 **SMB** 서버를 설정합니다

작업 그룹 개요에서 **SMB** 서버를 설정합니다

작업 그룹에서 SMB 서버를 구성원으로 설정하는 작업은 SMB 서버를 생성한 다음 로컬 사용자 및 그룹을 만드는 작업으로 구성됩니다.

Microsoft Active Directory 도메인 인프라를 사용할 수 없는 경우 작업 그룹에서 SMB 서버를 구성할 수 있습니다.

작업 그룹 모드의 SMB 서버는 NTLM 인증만 지원하며 Kerberos 인증을 지원하지 않습니다.

워크그룹에 **SMB** 서버를 생성합니다

"vserver cifs create" 명령을 사용하여 SVM에 SMB 서버를 생성하고 해당 서버가 속한 작업 그룹을 지정할 수 있습니다.

시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 SMB 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버에 연결할 수 있어야 합니다.

이 작업에 대해

워크그룹 모드의 SMB 서버는 다음 SMB 기능을 지원하지 않습니다.

- SMB3 Witness 프로토콜
- SMB3 CA 공유
- SMB를 통한 SQL
- 폴더 리디렉션
- 로밍 프로필
- GPO(그룹 정책 개체)
- VSS(볼륨 스냅샷 서비스)

'vserver cifs' man 페이지에는 추가 옵션 구성 매개 변수 및 명명 요구 사항이 포함되어 있습니다.

단계

1. smb 라이선스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

SMB 라이선스는 에 포함되어 있습니다 ["ONTAP 1 을 참조하십시오"](#). ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이선스가 필요하지 않습니다.

2. 워크그룹에서 SMB 서버를 생성합니다. 'vserver cifs create-vserver vserver\_name-cifs-server cifs\_server\_name-workgroup workgroup\_name[-comment text]'

다음 명령을 실행하면 워크그룹 workgroup01에 SMB 서버 "smb\_server01"이 생성됩니다.

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
SMB_SERVER01 -workgroup workgroup01
```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

다음 예제에서 명령 출력은 "workgroup01" 워크그룹의 SVM vs1.example.com 에서 "smb\_server01" 이름의 SMB 서버가 생성되었음을 보여 줍니다.

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

작업을 마친 후

작업 그룹의 CIFS 서버의 경우 SVM에서 로컬 사용자와 로컬 그룹을 생성해야 합니다(선택 사항).

관련 정보

["SMB 관리"](#)

로컬 사용자 계정을 생성합니다

SMB 연결을 통해 SVM에 포함된 데이터에 대한 액세스를 승인하는 데 사용할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. SMB 세션을 생성할 때 인증에 로컬 사용자 계정을 사용할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 사용자 기능이 기본적으로 활성화됩니다.

로컬 사용자 계정을 생성할 때 사용자 이름을 지정해야 하며 계정을 연결할 SVM을 지정해야 합니다.

'vserver cifs users-and-groups local-user' man 페이지에는 선택적 매개 변수 및 명명 요구 사항에 대한 세부 정보가 포함되어 있습니다.

단계

1. 로컬 사용자:'vserver cifs users-and-groups local-user create-vserver\_vserver\_name\_-user-name\_user\_name\_\_optional\_parameters\_'를 생성합니다

다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

- 이름

사용자의 전체 이름입니다.

- ``설명``

로컬 사용자에게 대한 설명입니다.

- '-is-account-disabled{true|false}'

사용자 계정의 사용 여부를 지정합니다. 이 매개 변수를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다.

명령을 실행하면 로컬 사용자 암호를 묻는 메시지가 표시됩니다.

2. 로컬 사용자의 암호를 입력한 다음 암호를 확인합니다.
3. 사용자가 성공적으로 생성되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver\_vserver\_name\_'

예

다음 예에서는 SVM vs1.example.com 과 관련된 "sUE Chang"이라는 전체 이름으로 로컬 사용자 "sMB\_SERVER01\sue"를 생성합니다.

```
cluster1::> vsserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vsserver cifs users-and-groups local-user show
Vserver   User Name                               Full Name   Description
-----
vs1       SMB_SERVER01\Administrator              Built-in administrator
account
vs1       SMB_SERVER01\sue                        Sue Chang
```

로컬 그룹을 생성합니다

SMB 연결을 통해 SVM과 관련된 데이터에 대한 액세스 권한을 부여하는 데 사용할 수 있는 로컬 그룹을 생성할 수 있습니다. 그룹의 구성원이 보유한 사용자 권한 또는 기능을 정의하는 권한을 할당할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 그룹 기능이 기본적으로 활성화됩니다.

로컬 그룹을 생성할 때 그룹 이름을 지정해야 하며 그룹을 연결할 SVM을 지정해야 합니다. 로컬 도메인 이름을 사용하거나 사용하지 않고 그룹 이름을 지정할 수 있으며, 선택적으로 로컬 그룹에 대한 설명을 지정할 수 있습니다. 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.

'vsserver cifs users-and-groups local-group' man 페이지에는 선택적 매개 변수 및 명명 요구 사항에 대한 세부 정보가

포함되어 있습니다.

#### 단계

1. 로컬 그룹 'vserver cifs users-and-groups local-group create-vserver vserver\_name-group-name group\_name'을 생성합니다

다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

- ``설명``

로컬 그룹에 대한 설명입니다.

2. 그룹이 성공적으로 생성되었는지 확인합니다. 'vserver cifs users-and-groups local-group show-vserver vserver\_name'

#### 예

다음 예에서는 SVM VS1 관련 로컬 그룹 "SMB\_SERVER01\engineering"을 생성합니다.

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

Vserver	Group Name	Description
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

작업을 마친 후

새 그룹에 구성원을 추가해야 합니다.

로컬 그룹 구성원 자격을 관리합니다

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 구성원 자격을 관리할 수 있습니다. 이 기능은 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하려는 경우 또는 사용자가 해당 그룹에 연결된 권한을 가지도록 하려는 경우에 유용합니다.

이 작업에 대해

더 이상 로컬 사용자, 도메인 사용자 또는 도메인 그룹이 그룹의 구성원 자격에 따라 액세스 권한이나 권한을 가지도록 하지 않으려면 그룹에서 해당 구성원을 제거할 수 있습니다.

로컬 그룹에 구성원을 추가할 때는 다음 사항을 염두에 두어야 합니다.

- special\_everyone\_group에 사용자를 추가할 수 없습니다.
- 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.
- 도메인 사용자 또는 그룹을 로컬 그룹에 추가하려면 ONTAP에서 SID에 대한 이름을 확인할 수 있어야 합니다.

로컬 그룹에서 구성원을 제거할 때는 다음 사항을 염두에 두어야 합니다.

- special\_everyone\_group에서 구성원을 제거할 수 없습니다.
- 로컬 그룹에서 구성원을 제거하려면 ONTAP에서 해당 이름을 SID로 확인할 수 있어야 합니다.

## 단계

### 1. 그룹에 구성원을 추가하거나 그룹에서 구성원을 제거합니다.

- 멤버(+ vserver cifs users-and-groups local-group add-member -vserver\_name -group-name group\_name -member-name name[...]+')를 추가합니다

로컬 사용자, 도메인 사용자 또는 도메인 그룹의 심표로 구분된 목록을 지정하여 지정된 로컬 그룹에 추가할 수 있습니다.

- 멤버(+ vserver cifs users-and-groups local-group remove-member-vserver vserver\_name -group-name group\_name -member-name[...]+')를 제거합니다

로컬 사용자, 도메인 사용자 또는 도메인 그룹의 심표로 구분된 목록을 지정하여 지정된 로컬 그룹에서 제거할 수 있습니다.

## 예

다음 예에서는 SVM vs1.example.com 에서 로컬 사용자 "sMB\_SERVER01\SUB"를 로컬 그룹 "sMB\_SERVER01\engineering"에 추가합니다.

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

다음 예에서는 SVM vs1.example.com 에서 로컬 그룹 "sMB\_SERVER01\engineering"에서 로컬 사용자 "sMB\_SERVER01\SUB" 및 "sMB\_SERVER01\James"를 제거합니다.

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

## 활성화된 **SMB** 버전을 확인합니다

ONTAP 9 릴리즈에서는 클라이언트 및 도메인 컨트롤러와의 연결에 대해 기본적으로 설정되는 SMB 버전을 결정합니다. SMB 서버가 사용자 환경에 필요한 클라이언트 및 기능을 지원하는지 확인해야 합니다.

이 작업에 대해

클라이언트 및 도메인 컨트롤러 모두에 연결하는 경우 가능하면 SMB 2.0 이상을 활성화해야 합니다. 보안상의 이유로 SMB 1.0은 사용하지 않는 것이 좋습니다. 사용자 환경에서 필요하지 않은 것으로 확인된 경우에는 사용하지 않도록 설정해야 합니다.

ONTAP 9에서는 SMB 버전 2.0 이상이 클라이언트 연결에 대해 기본적으로 활성화되어 있지만 기본적으로 활성화되어 있는 SMB 1.0 버전은 ONTAP 릴리스에 따라 다릅니다.

- ONTAP 9.1 P8부터 SMB 1.0을 SVM에서 비활성화할 수 있습니다.

vserver cifs options modify 명령에 대한 '-SMB1-enabled' 옵션은 SMB 1.0을 활성화하거나 비활성화합니다.

- ONTAP 9.3부터는 새 SVM에서 기본적으로 비활성화되어 있습니다.

SMB 서버가 AD(Active Directory) 도메인에 있는 경우 SMB 2.0이 ONTAP 9.1부터 시작하는 DC(도메인 컨트롤러)에 연결되도록 설정할 수 있습니다. DC에서 SMB 1.0을 사용하지 않도록 설정한 경우 이 작업이 필요합니다. ONTAP 9.2부터는 SMB 2.0이 DC 연결에 대해 기본적으로 사용하도록 설정됩니다.



SMB1-enabled-for-dc-connections가 false로 설정되어 있고 -SMB1-enabled가 true로 설정되어 있으면 ONTAP는 SMB 1.0 연결을 클라이언트로 거부하지만 인바운드 SMB 1.0 연결을 서버로 계속 허용합니다.

"SMB 관리" 지원되는 SMB 버전 및 기능에 대한 자세한 내용은 에 나와 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 활성화된 SMB 버전을 확인합니다.

```
vserver cifs options show
```

목록을 아래로 스크롤하여 클라이언트 연결에 대해 설정된 SMB 버전을 볼 수 있으며 AD 도메인 연결에 대해 AD 도메인에서 SMB 서버를 구성하는 경우

3. 필요에 따라 클라이언트 연결에 대해 SMB 프로토콜을 설정하거나 해제합니다.

- SMB 버전 활성화하기:

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs options modify -vserver vserver_name smb_version false
```



에 사용할 수 있는 값 smb\_version:

- '-SMB1-활성화됨'
- '-SMB2-ENABLED'입니다
- '-SMB3-enabled'입니다
- -smb31-enabled

다음 명령을 실행하면 SVM vs1.example.com 에서 SMB 3.1이 활성화됩니다.

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. SMB 서버가 Active Directory 도메인에 있는 경우 필요에 따라 DC 연결에 대한 SMB 프로토콜을 설정하거나 해제합니다.

- SMB 버전 활성화하기:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

## 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.

## 공유 스토리지에 대한 **SMB** 클라이언트 액세스를 구성합니다

공유 스토리지에 대한 **SMB** 클라이언트 액세스를 구성합니다

SVM에서 공유 스토리지에 SMB 클라이언트가 액세스할 수 있도록 하려면 스토리지 컨테이너를 제공할 볼륨 또는 **qtree**를 생성한 다음 해당 컨테이너에 대한 공유를 생성하거나 수정해야 합니다. 그런 다음 공유 및 파일 권한을 구성하고 클라이언트 시스템에서 액세스를 테스트할 수 있습니다.

시작하기 전에

- SVM에서 SMB를 완전히 설정해야 합니다.
- 이름 서비스 구성에 대한 모든 업데이트를 완료해야 합니다.
- Active Directory 도메인 또는 작업 그룹 구성에 대한 추가 또는 수정 작업을 완료해야 합니다.

볼륨 또는 **qtree** 스토리지 컨테이너를 생성합니다

볼륨을 생성합니다

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

이 작업에 대해

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

시작하기 전에

- SMB를 설정하고 실행해야 합니다.
- SVM 보안 스타일은 NTFS여야 합니다.
- ONTAP 9.13.1 부터는 용량 분석 및 활동 추적 기능이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 명령을 사용하여 `-analytics-state` 또는 `-activity-tracking-state`를 `on`로 설정합니다.

용량 분석 및 활동 추적에 대한 자세한 내용은 [을 참조하십시오 파일 시스템 분석 설정.](#)

## 단계

1. 교차점으로 볼륨을 생성합니다. `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path`

'-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 '/existing\_dir/new\_vol' 등이 있습니다

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"과 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.

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
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

다음 명령을 실행하면 SVM의 "'home4" vs1.example.com`"'와 애그리게이트 "'aggr1"'에 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
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

**qtree**를 생성합니다

'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 NTFS여야 하며 SMB를 설정하고 실행해야 합니다.

단계

1. qtree: 'volume qtree create-vserver vserver\_name{-volume volume\_name-qtree qtree\_name|-qtree-path qtree path qtree path}-security-style NTFS'를 생성합니다

볼륨과 qtree를 별도의 인수로 지정하거나 qtree 경로 인수를 '/vol/volume\_name/\_qtree\_name' 형식으로 지정할 수 있습니다.

2. qtree가 'volume qtree show-vserver vserver\_name{-volume volume\_name-qtree qtree\_name|-qtree-path qtree path}' 접합 경로로 생성되었는지 확인합니다

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 ntfs  
[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: ntfs  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

## SMB 공유를 생성하기 위한 요구 사항 및 고려 사항

SMB 공유를 생성하기 전에 공유 경로 및 공유 속성, 특히 홈 디렉토리에 대한 요구 사항을 이해해야 합니다.

SMB 공유를 생성하려면 클라이언트가 액세스할 디렉토리 경로 구조('vserver cifs share create' 명령의 '-path' 옵션 사용)를 지정해야 합니다. 디렉토리 경로는 SVM 네임스페이스에서 생성한 볼륨 또는 qtree의 접합 경로에 해당합니다. 공유를 생성하기 전에 디렉토리 경로 및 해당 접속 경로가 있어야 합니다.

공유 경로에는 다음과 같은 요구 사항이 있습니다.

- 디렉터리 경로 이름은 최대 255자까지 지정할 수 있습니다.
- 경로 이름에 공백이 있으면 전체 문자열을 따옴표로 묶어야 합니다(예: "/new volume/mount here").
- 공유의 UNC 경로("\\servername\sharename\filepath")에 256자 이상(UNC 경로의 초기 "\\\" 제외)이 포함되어 있으면 Windows 속성 상자의 \* Security \* 탭을 사용할 수 없습니다.

이것은 ONTAP 문제가 아니라 Windows 클라이언트 문제입니다. 이 문제를 방지하려면 256자를 초과하는 UNC 경로를 사용하여 공유를 생성하지 마십시오.

공유 속성 기본값은 다음과 같이 변경할 수 있습니다.

- 모든 주식의 기본 초기 속성은 oplocks, 탐색 가능, 변경 및 이전 버전 사용입니다.
- 공유를 생성할 때 공유 속성을 지정하는 것은 선택 사항입니다.

그러나 공유를 생성할 때 공유 속성을 지정하면 기본값이 사용되지 않습니다. 공유를 만들 때 '-share-properties' 매개 변수를 사용하는 경우 쉼표로 구분된 목록을 사용하여 공유에 적용할 모든 공유 속성을 지정해야 합니다.

- 홈 디렉토리 공유를 지정하려면 홈 디렉토리 속성을 사용합니다.

이 기능을 사용하면 연결된 사용자와 변수 집합을 기반으로 서로 다른 디렉토리에 매핑되는 공유를 구성할 수 있습니다. 사용자별로 별도의 공유를 생성할 필요 없이 몇 가지 홈 디렉토리 매개 변수를 사용하여 단일 공유를 구성하여 엔트리 포인트(공유)와 해당 홈 디렉토리(SVM의 디렉토리) 간의 사용자 관계를 정의할 수 있습니다.



공유를 생성한 후에는 이 속성을 추가하거나 제거할 수 없습니다.

홈 디렉토리 공유에는 다음과 같은 요구 사항이 있습니다.

- SMB 홈 디렉토리를 생성하기 전에 'vserver cifs home-directory search-path add' 명령을 사용하여 적어도 하나의 홈 디렉토리 검색 경로를 추가해야 합니다.
- '-share-properties' 파라미터의 homed디렉토리 값으로 지정된 홈 디렉토리 공유에는 공유 이름에 '%w'(Windows 사용자 이름) 동적 변수가 포함되어야 합니다.

공유 이름에는 "%d"(도메인 이름) 동적 변수(예: "%d/%w") 또는 공유 이름의 정적 부분(예: "home1\_%w")이 추가로 포함될 수 있습니다.

- 관리자 또는 사용자가 공유를 사용하여 다른 사용자의 홈 디렉토리에 연결하는 경우('vserver cifs home-directory modify' 명령 옵션 사용) 동적 공유 이름 패턴 앞에는 물결표('~')가 와야 합니다.

"SMB 관리" 그리고 'vserver cifs share' man 페이지에 추가 정보가 있습니다.

## SMB 공유를 생성합니다

SMB 클라이언트와 SMB 서버의 데이터를 공유하려면 먼저 SMB 공유를 생성해야 합니다. 공유를 생성할 때 공유를 홈 디렉토리로 지정하는 등의 공유 속성을 설정할 수 있습니다. 선택적 설정을 구성하여 공유를 사용자 지정할 수도 있습니다.

시작하기 전에

공유를 생성하기 전에 SVM 네임스페이스에 볼륨 또는 qtree의 디렉토리 경로가 있어야 합니다.

이 작업에 대해

공유를 생성할 때 기본 공유 ACL(기본 공유 권한)은 '모든 사용자/모든 권한'입니다. 공유에 대한 액세스를 테스트한 후에는 기본 공유 ACL을 제거하고 보다 안전한 대체 공유 ACL로 대체해야 합니다.

단계

1. 필요한 경우 공유에 대한 디렉토리 경로 구조를 생성합니다.

'vserver cifs share create' 명령은 공유 생성 중에 '-path' 옵션에 지정된 경로를 확인합니다. 지정한 경로가 없으면 명령이 실패합니다.

2. 지정된 SVM과 연결된 SMB 공유 생성: "+ vserver cifs share create -vserver vserver\_name -share-name share\_name -path path [-share-properties share\_properties,...] [Other\_attributes] [-comment text]+"
3. 공유가 생성되었는지 확인합니다. "vserver cifs share show-share-name share\_name"

예

다음 명령을 실행하면 SVM vs1.example.com "sSHARE1"이라는 SMB 공유가 생성됩니다. 디렉터리 경로는 '/users'이며 기본 속성으로 만들어집니다.

```
cluster1::> vsriver cifs share create -vsriver vs1.example.com -share-name SHARE1 -path /users
```

```
cluster1::> vsriver cifs share show -share-name SHARE1
```

Vsriver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

## 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.

## SMB 공유 액세스 제어 목록을 생성합니다

SMB 공유에 대한 ACL(액세스 제어 목록)을 생성하여 공유 권한을 구성하면 사용자 및 그룹의 공유에 대한 액세스 수준을 제어할 수 있습니다.

시작하기 전에

공유에 대한 액세스 권한을 부여할 사용자 또는 그룹을 결정해야 합니다.

이 작업에 대해

로컬 또는 도메인 Windows 사용자 또는 그룹 이름을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

새 ACL을 생성하기 전에 보안 위험을 야기시키는 기본 공유 ACL 'Everyone/Full Control'을 삭제해야 합니다.

워크그룹 모드에서 로컬 도메인 이름은 SMB 서버 이름입니다.

단계

1. 기본 공유 ACL: ``vserver cifs share access-control delete-vserver\_vserver\_name\_-share\_share\_name\_-user-or-group everyone"을 삭제합니다
2. 새 ACL 구성:

을 사용하여 <b>ACL</b> 을 구성하려면...	명령 입력...
Windows 사용자	'vserver cifs share access-control create-vserver_name_-share_share_name_-user-group-type windows-user-or-group_windows_domain_name\\user_name_-permission access_right'
Windows 그룹	'vserver cifs share access-control create-vserver_name_-share_share_name_-user-group-type windows-user-or-group_windows_group_name_-permission access_right'

3. 'vserver cifs share access-control show' 명령을 사용하여 공유에 적용된 ACL이 올바른지 확인하십시오.

예

다음 명령을 실행하면 vs1.example.com`"SVM: "Sales" 공유에 대한 "Sales Team" Windows 그룹에 대한 "Change" 권한이 부여됩니다

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show

Vserver      Share      User/Group      User/Group  Access
Permission   Name       Name            Type
-----
vs1.example.com  c$        BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales     DOMAIN\"Sales Team"    windows      Change
```

다음 명령은 로컬 윈도우 그룹인 '타이거 팀'과 'Full\_Control'에 대한 'SUE Chang'이라는 이름의 변경 권한을 VS1 SVM의 'datavol5' 공유에 부여합니다.



```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\ "Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\ "Sue Chang"	windows	Full_Control

## 공유에서 **NTFS** 파일 권한을 구성합니다

공유에 대한 액세스 권한이 있는 사용자 또는 그룹에 대한 파일 액세스를 설정하려면 Windows 클라이언트에서 공유하는 파일 및 디렉토리에 대한 NTFS 파일 권한을 구성해야 합니다.

시작하기 전에

이 작업을 수행하는 관리자는 선택한 개체에 대한 권한을 변경할 수 있는 충분한 NTFS 권한이 있어야 합니다.

이 작업에 대해

**"SMB 관리"** 및 Windows 설명서에는 표준 및 고급 NTFS 권한을 설정하는 방법에 대한 정보가 포함되어 있습니다.

단계

1. Windows 클라이언트에 관리자로 로그인합니다.
2. Windows 탐색기의 \* Tools \* 메뉴에서 \* Map network drive \* 를 선택합니다.
3. 네트워크 드라이브 매핑 \* 상자를 완료합니다.
  - a. 드라이브 \* 문자를 선택합니다.
  - b. 폴더 \* 상자에 사용 권한을 적용할 데이터와 공유 이름을 포함하는 공유가 포함된 SMB 서버 이름을 입력합니다.

SMB 서버 이름이 smb\_SERVER01이고 공유 이름이 "smb\_SERVER01"이면  
 "\\smb\_SERVER01\share1"을 입력합니다.



SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

c. 마침 \* 을 클릭합니다.

선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

4. NTFS 파일 권한을 설정할 파일 또는 디렉터리를 선택합니다.

5. 파일 또는 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 \* 속성 \* 을 선택합니다.

6. 보안 \* 탭을 선택합니다.

보안 탭에는 NTFS 권한이 설정된 사용자 및 그룹 목록이 표시됩니다. Object>에 대한 권한 상자에는 선택한 사용자 또는 그룹에 적용되는 허용 및 거부 권한 목록이 표시됩니다.

7. 편집 \* 을 클릭합니다.

Object> 사용 권한 상자가 열립니다.

8. 원하는 작업을 수행합니다.

원하는 경우	다음을 수행합니다.
새 사용자 또는 그룹에 대한 표준 NTFS 권한을 설정합니다	a. 추가 * 를 클릭합니다.  사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 창이 열립니다.  b. 선택할 개체 이름 입력 * 상자에 NTFS 권한을 추가할 사용자 또는 그룹의 이름을 입력합니다.  c. 확인 * 을 클릭합니다.
사용자 또는 그룹에서 표준 NTFS 권한을 변경하거나 제거합니다	그룹 또는 사용자 이름 * 상자에서 변경하거나 제거할 사용자 또는 그룹을 선택합니다.

9. 원하는 작업을 수행합니다.

원하는 작업	다음을 수행합니다
새 사용자 또는 기존 사용자 또는 그룹에 대해 표준 NTFS 권한을 설정합니다	Object>*에 대한 권한 상자에서 선택한 사용자 또는 그룹에 대해 허용하거나 허용하지 않을 액세스 유형에 대해 * 허용 * 또는 * 거부 * 상자를 선택합니다.
사용자 또는 그룹을 제거합니다	제거 * 를 클릭합니다.



일부 또는 모든 표준 권한 상자를 선택할 수 없는 경우 상위 개체에서 사용 권한이 상속되기 때문입니다. 특수 권한 \* 상자는 선택할 수 없습니다. 이 옵션을 선택하면 선택한 사용자 또는 그룹에 대해 하나 이상의 세분화된 고급 권한이 설정되었음을 의미합니다.

10. 해당 개체에 대한 NTFS 권한을 추가, 제거 또는 편집한 후 \* 확인 \* 을 클릭합니다.

## 사용자 액세스를 확인합니다

구성한 사용자가 SMB 공유 및 해당 공유에 포함된 파일에 액세스할 수 있는지 테스트해야 합니다.

### 단계

1. Windows 클라이언트에서 공유에 대한 액세스 권한이 있는 사용자 중 하나로 로그인합니다.
2. Windows 탐색기의 \* Tools \* 메뉴에서 \* Map network drive \* 를 선택합니다.
3. 네트워크 드라이브 매핑 \* 상자를 완료합니다.

a. 드라이브 \* 문자를 선택합니다.

b. 폴더 \* 상자에 사용자에게 제공할 공유 이름을 입력합니다.

SMB 서버 이름이 smb\_SERVER01이고 공유 이름이 "smb\_SERVER01"이면  
"\\smb\_SERVER01\share1"을 입력합니다.

c. 마침 \* 을 클릭합니다.

선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

4. 테스트 파일을 만들고, 파일이 있는지 확인하고, 텍스트를 작성한 다음 테스트 파일을 제거합니다.

## 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

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