



# 공유 스토리지에 대한 **SMB** 클라이언트 액세스를 구성합니다 ONTAP 9

NetApp  
April 24, 2024

# 목차

공유 스토리지에 대한 SMB 클라이언트 액세스를 구성합니다 .....	1
공유 스토리지에 대한 SMB 클라이언트 액세스를 구성합니다 .....	1
볼륨 또는 qtree 스토리지 컨테이너를 생성합니다 .....	1
SMB 공유를 생성하기 위한 요구 사항 및 고려 사항 .....	3
SMB 공유를 생성합니다 .....	4
SMB 클라이언트 액세스를 확인합니다 .....	5
SMB 공유 액세스 제어 목록을 생성합니다 .....	6
공유에서 NTFS 파일 권한을 구성합니다 .....	7
사용자 액세스를 확인합니다 .....	9

# 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 사용합니다 `-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

## qtree를 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 "sHARE1"이라는 SMB 공유가 생성됩니다. 디렉터리 경로는 '/users'이며 기본 속성으로 만들어집니다.

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

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

Vserver	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 '\\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::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsserver cifs share access-control show
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
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::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

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

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

Vserver	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	<ol style="list-style-type: none"><li>a. 추가 * 를 클릭합니다.  사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 창이 열립니다.</li><li>b. 선택할 개체 이름 입력 * 상자에 NTFS 권한을 추가할 사용자 또는 그룹의 이름을 입력합니다.</li><li>c. 확인 * 을 클릭합니다.</li></ol>
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.