



# CLI를 사용하여 SMB를 관리합니다

## ONTAP 9

NetApp  
April 24, 2024

# 목차

CLI를 사용하여 SMB를 관리합니다 .....	1
SMB 참조 개요 .....	1
SMB 서버 지원 .....	1
SMB 서버를 관리합니다 .....	8
SMB를 사용하여 파일 액세스를 설정합니다 .....	100
SMB를 사용하여 파일 액세스를 관리합니다 .....	164
SMB 클라이언트 기반 서비스 구축 .....	251
SMB 서버 기반 서비스 구축 .....	264
NFS 및 SMB 파일 및 디렉토리 명명 종속성 .....	328

# CLI를 사용하여 SMB를 관리합니다

## SMB 참조 개요

SMB 프로토콜에서 ONTAP 파일 액세스 기능을 사용할 수 있습니다. CIFS 서버를 설정하고, 공유를 생성하고, Microsoft 서비스를 설정할 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 상황에서 이러한 절차를 사용해야 합니다.

- ONTAP SMB 프로토콜 기능의 범위를 이해하려고 합니다.
- 기본적인 SMB 구성이 아닌, 덜 일반적인 구성 및 유지 관리 작업을 수행해야 합니다.
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

## SMB 서버 지원

### SMB 서버 지원 개요

SMB 클라이언트가 클러스터의 파일에 액세스할 수 있도록 SVM(스토리지 가상 머신)에서 SMB 서버를 설정 및 구성할 수 있습니다.

- 클러스터의 각 데이터 SVM은 하나의 Active Directory 도메인에 정확히 바인딩할 수 있습니다.
- Data SVM을 동일한 도메인에 연결할 필요가 없습니다.
- 여러 SVM을 동일한 도메인에 바인딩할 수 있습니다.

SMB 서버를 생성하기 전에 데이터 제공을 위해 사용 중인 SVM 및 LIF를 구성해야 합니다. 데이터 네트워크가 편평하지 않은 경우 IPspace, 브로드캐스트 도메인 및 서브넷을 구성해야 할 수도 있습니다. 자세한 내용은 *\_Network Management Guide\_*를 참조하십시오.

관련 정보

["네트워크 관리"](#)

[SMB 서버를 수정합니다](#)

["시스템 관리"](#)

### 지원되는 SMB 버전 및 기능

SMB(Server Message Block)는 Microsoft Windows 클라이언트 및 서버에서 사용하는 원격 파일 공유 프로토콜입니다. ONTAP 9에서는 모든 SMB 버전이 지원되지만, 기본 SMB 1.0 지원은 ONTAP 버전에 따라 다릅니다. ONTAP SMB 서버가 사용자 환경에 필요한 클라이언트 및 기능을 지원하는지 확인해야 합니다.

ONTAP가 지원하는 SMB 클라이언트 및 도메인 컨트롤러에 대한 최신 정보는 \_Interoperability Matrix Tool\_에서 확인할 수 있습니다.

SMB 2.0 이상 버전은 ONTAP 9 SMB 서버에 대해 기본적으로 활성화되어 있으며 필요에 따라 활성화하거나 비활성화할 수 있습니다. 다음 표에서는 SMB 1.0 지원 및 기본 구성을 보여 줍니다.

<b>SMB 1.0 기능:</b>	<b>ONTAP 9 릴리스의 경우:</b>			
	9.0	9.1	9.2	9.3 이상
기본적으로 사용하도록 설정되어 있습니다	예	예	예	아니요
활성화 또는 비활성화할 수 있습니다	아니요	예 * 9.1 P8 이상 필요.	예	예



도메인 컨트롤러에 대한 SMB 1.0 및 2.0 연결의 기본 설정은 ONTAP 버전에도 따라 다릅니다. 자세한 내용은 SVM CIFS 보안 수정 man 페이지를 참조하십시오. SMB 1.0을 실행하는 기존 CIFS 서버가 있는 환경의 경우 보안 및 규정 준수 향상을 준비하기 위해 가능한 한 빨리 최신 SMB 버전으로 마이그레이션해야 합니다. 자세한 내용은 NetApp 담당자에게 문의하십시오.

다음 표에서는 각 SMB 버전에서 지원되는 SMB 기능을 보여 줍니다. 일부 SMB 기능은 기본적으로 활성화되어 있으며 일부는 추가 구성이 필요합니다.

* 이 기능은 * 입니다	* 지원 필요: *	* 는 다음 <b>SMB</b> 버전에 대해 <b>ONTAP 9</b> 에서 지원됩니다. *				
		1.0	2.0	2.1	3.0	3.1.1
레거시 SMB 1.0 기능		X	X	X	X	X
내구성이 뛰어난 핸들			X	X	X	X
결합 작업			X	X	X	X
비동기 작업			X	X	X	X
읽기 및 쓰기 버퍼 크기가 증가되었습니다			X	X	X	X
확장성 향상			X	X	X	X
SMB 서명	X	X	X	X	X	X

* 이 기능은 * 입니다	* 지원 필요: *	* 는 다음 <b>SMB</b> 버전에 대해 <b>ONTAP 9</b> 에서 지원됩니다. *				
ADS(대체 데이터 스트림) 파일 형식입니다	X	X	X	X	X	X
Large MTU(ONTAP 9.7부터 기본적으로 활성화됨)	X			X	X	X
oplocks 리스				X	X	X
지속적으로 사용 가능한 공유	X				X	X
영구 핸들					X	X
증인					X	X
SMB 암호화: AES-128- CCM	X				X	X
스케일아웃(CA 공유에 필요)					X	X
투명한 페일오버					X	X
SMB 멀티 채널(ONTAP 9.4로 시작)	X				X	X
사전 인증 무결성						X
클러스터 클라이언트 페일오버 v.2(CCFv2)						X

* 이 기능은 * 입니다	* 지원 필요: *	* 는 다음 <b>SMB</b> 버전에 대해 <b>ONTAP 9</b> 에서 지원됩니다. *				
SMB 암호화: AES-128- GCM(ONTAP 9.1부터 시작)	X					X

관련 정보

[SMB 서명을 사용하여 네트워크 보안을 강화합니다](#)

[SMB 서버 최소 인증 보안 수준 설정](#)

[SMB를 통한 데이터 전송을 위해 SMB 서버에서 필요한 SMB 암호화 구성](#)

["NetApp 기술 보고서 4543: SMB 프로토콜 모범 사례"](#)

["NetApp 상호 운용성"](#)

지원되지 않는 **Windows** 기능입니다

네트워크에서 CIFS를 사용하기 전에 ONTAP에서 지원하지 않는 특정 Windows 기능을 알고 있어야 합니다.

ONTAP는 다음 Windows 기능을 지원하지 않습니다.

- 암호화된 파일 시스템(EFS)
- 변경 저널에서 NTFS(NT File System) 이벤트 로깅
- Microsoft FRS(파일 복제 서비스)
- Microsoft Windows 인덱싱 서비스
- HSM(Hierarchical Storage Management)을 통한 원격 스토리지
- Windows 클라이언트의 할당량 관리
- Windows 할당량 의미 체계입니다
- LMHOSTS 파일입니다
- NTFS 네이티브 압축

**SVM**에서 **NIS** 또는 **LDAP** 네임 서비스를 구성합니다

SMB 액세스를 사용하면 NTFS 보안 스타일 볼륨에서 데이터에 액세스할 때도 UNIX 사용자에게 대한 사용자 매핑이 항상 수행됩니다. 정보가 NIS 또는 LDAP 디렉토리 저장소에 저장되어 있는 해당 UNIX 사용자에게 Windows 사용자를 매핑하거나 이름 매핑에 LDAP를 사용하는 경우 SMB 설정 중에 이러한 이름 서비스를 구성해야 합니다.

시작하기 전에

네임 서비스 데이터베이스 구성을 네임 서비스 인프라에 맞게 사용자 지정해야 합니다.

## 이 작업에 대해

SVM은 이름 서비스 ns-switch 데이터베이스를 사용하여 지정된 이름 서비스 데이터베이스의 소스를 조회하는 순서를 결정합니다. ns-switch 소스는 "파일", "NIS" 또는 "LDAP" 중 어떤 조합도 가능합니다. 그룹 데이터베이스의 경우 ONTAP은 구성된 모든 소스에서 그룹 구성원 자격을 얻은 다음 통합된 그룹 구성원 정보를 사용하여 액세스 검사를 수행합니다. UNIX 그룹 정보를 가져올 때 이러한 소스 중 하나를 사용할 수 없는 경우 ONTAP에서 전체 UNIX 자격 증명을 가져올 수 없으며 이후의 액세스 검사에 실패할 수 있습니다. 따라서 항상 ns-switch 설정에서 그룹 데이터베이스에 대해 모든 ns-switch 소스가 구성되어 있는지 확인해야 합니다.

기본값은 SMB 서버가 모든 Windows 사용자를 로컬 'passwd' 데이터베이스에 저장된 기본 UNIX 사용자에게 매핑하도록 하는 것입니다. 기본 구성을 사용하려면 NIS 또는 LDAP UNIX 사용자 및 그룹 이름 서비스 구성 또는 LDAP 사용자 매핑은 SMB 액세스에 대해 선택 사항입니다.

## 단계

1. UNIX 사용자, 그룹 및 넷그룹 정보가 NIS 이름 서비스를 통해 관리되는 경우 NIS 이름 서비스를 구성합니다.
  - a. 'vserver services name-service ns-switch show' 명령을 사용하여 이름 서비스의 현재 순서를 확인합니다.

이 예에서는 NIS를 이름 서비스 소스로 사용할 수 있는 세 개의 데이터베이스(group, passwd, netgroup)가 파일(file)만 소스로 사용하고 있습니다.

'vserver services name-service ns-switch show-vserver vs1'

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

그룹 및 암호 데이터베이스에 NIS 소스를 추가하고 선택적으로 넷그룹 데이터베이스에 추가해야 합니다.

- b. 'vserver services name-service ns-switch modify' 명령을 사용하여 이름 서비스 ns-switch 데이터베이스 순서를 원하는 대로 조정합니다.

최상의 성능을 위해 SVM에서 네임 서비스를 구성하려는 경우를 제외하고 네임 서비스 데이터베이스에 네임 서비스를 추가할 수 없습니다.

둘 이상의 이름 서비스 데이터베이스에 대한 구성을 수정하는 경우 수정할 각 이름 서비스 데이터베이스에 대해 명령을 별도로 실행해야 합니다.

이 예에서 NIS와 파일은 그룹 데이터베이스와 암호 데이터베이스의 소스로 구성됩니다. 나머지 이름 서비스 데이터베이스는 변경되지 않습니다.

```
'vserver services name-service ns-switch modify -vserver vs1 -database group -sources nis, files'
vserver services name-service ns-switch modify -vserver vs1-database passwd-sources nis, files'
```

- c. 'vserver services name-service ns-switch show' 명령을 사용하여 이름 서비스의 순서가 올바른지

확인합니다.

```
'vserver services name-service ns-switch show-vserver vs1'
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

- d. NIS 이름 서비스 구성을 생성합니다. + 'vserver services name-service NIS-domain create-vserver\_vserver\_name\_-domain\_NIS\_domain\_name\_-servers\_NIS\_server\_IPaddress\_,... -active true+'입니다

```
'vserver services name-service NIS-domain create-vserver vs1-domain example.com -servers 10.0.0.60 -active true'
```



ONTAP 9.2부터, 필드 '-NIS-SERS'는 필드 '-SERVers'를 대체합니다. 이 새 필드는 NIS 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

- e. NIS 이름 서비스가 올바르게 구성되어 활성화되어 있는지 확인합니다. 'vserver services name-service nis-domain show vserver\_vserver\_name\_'

```
'vserver services name-service nis-domain show vserver vs1'
```

Vserver	Domain	Active	Server
vs1	example.com	true	10.0.0.60

2. UNIX 사용자, 그룹 및 넷그룹 정보 또는 이름 매핑이 LDAP 이름 서비스에 의해 관리되는 경우 찾은 정보를 사용하여 LDAP 이름 서비스를 구성합니다 ["NFS 관리"](#).

## ONTAP 네임 서비스 스위치 구성의 작동 방식

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다. 환경에 맞게 적절하게 구성할 수 있도록 표의 기능과 ONTAP에서 표의 사용 방법을 이해해야 합니다.

ONTAP 이름 서비스 스위치 테이블은 ONTAP가 특정 유형의 이름 서비스 정보에 대한 정보를 검색하기 위해 어떤 이름 서비스 소스를 참조합니다. ONTAP는 SVM별로 개별 네임 서비스 스위치 테이블을 유지 관리합니다.



## 데이터베이스 유형

이 테이블에는 다음과 같은 각 데이터베이스 유형에 대해 별도의 이름 서비스 목록이 저장됩니다.

데이터베이스 유형입니다	다음에 대한 이름 서비스 소스를 정의합니다.	유효한 소스는...
호스트	호스트 이름을 IP 주소로 변환	파일, DNS
그룹	사용자 그룹 정보를 찾는 중입니다	파일, NIS, LDAP
암호	사용자 정보를 찾는 중입니다	파일, NIS, LDAP
넷그룹	넷그룹 정보를 찾는 중입니다	파일, NIS, LDAP
이름맵	사용자 이름 매핑 중	파일, LDAP

## 소스 유형

소스는 해당 정보를 검색하는 데 사용할 이름 서비스 소스를 지정합니다.

원본 유형 지정...	에서 정보를 조회하려면...	관리 대상 명령 제품군...
파일	로컬 소스 파일	SVM 서비스 이름 서비스 유닉스 사용자 SVM 서비스 이름 서비스 유닉스 그룹  SVM 서비스 이름 서비스 넷그룹  SVM 서비스 이름-서비스 DNS 호스트
NIS를 선택합니다	SVM의 NIS 도메인 구성에 지정된 외부 NIS 서버	'vserver services name-service nis- domain'을 선택합니다
LDAP를 지원합니다	SVM의 LDAP 클라이언트 구성에 지정된 외부 LDAP 서버	'vserver services name-service ldap'
DNS	SVM의 DNS 구성에 지정된 외부 DNS 서버	SVM 서비스 이름-서비스 DNS

데이터 액세스와 SVM 관리 인증 모두에 NIS 또는 LDAP를 사용하려는 경우에도 NIS 또는 LDAP 인증이 실패할 경우 "파일"을 포함하고 로컬 사용자를 대체 수단으로 구성해야 합니다.

외부 소스에 액세스하는 데 사용되는 프로토콜입니다

외부 소스의 서버에 액세스하기 위해 ONTAP는 다음 프로토콜을 사용합니다.

외부 이름 서비스 소스입니다	액세스에 사용되는 프로토콜입니다
NIS를 선택합니다	UDP입니다
DNS	UDP입니다
LDAP를 지원합니다	TCP

예

다음 예는 SVM의 VM\_1'에 대한 이름 서비스 스위치 구성을 표시합니다.

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source Order
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

사용자 또는 그룹 정보를 조회하기 위해 ONTAP은 로컬 소스 파일만 참조합니다. 쿼리가 결과를 반환하지 않으면 조회가 실패합니다.

넷그룹 정보를 조회하기 위해 ONTAP은 먼저 외부 NIS 서버를 참조합니다. 쿼리가 결과를 반환하지 않으면 로컬 넷그룹 파일이 다음에 선택됩니다.

SVM svm\_1의 테이블에는 이름 매핑에 대한 이름 서비스 항목이 없습니다. 따라서 ONTAP은 기본적으로 로컬 소스 파일만 참조합니다.

## SMB 서버를 관리합니다

### SMB 서버를 수정합니다

"vserver cifs modify" 명령을 사용하여 작업 그룹에서 Active Directory 도메인으로, 작업 그룹에서 다른 작업 그룹으로 또는 Active Directory 도메인에서 작업 그룹으로 SMB 서버를 이동할 수 있습니다.

이 작업에 대해

SMB 서버 이름 및 관리 상태와 같은 SMB 서버의 다른 속성을 수정할 수도 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

선택

- 작업 그룹에서 Active Directory 도메인으로 SMB 서버 이동:
  - SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. 작업 그룹에서 Active Directory 도메인으로 SMB 서버를 이동합니다: 'vserver cifs modify -vserver\_vserver\_name\_-domain\_domain\_name\_'

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 'example'.com 도메인 내의 'ou=\_example\_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

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.

- 작업 그룹에서 다른 작업 그룹으로 SMB 서버 이동:
  - a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMB 서버의 워크그룹을 수정합니다. 'vserver cifs modify -vserver\_vserver\_name\_-workgroup\_new\_workgroup\_name\_'

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory 도메인에서 작업 그룹으로 SMB 서버 이동:
  - a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMB 서버를 Active Directory 도메인에서 작업 그룹('vserver cifs modify -vserver\_vserver\_name\_-workgroup\_workgroup\_name\_')으로 이동합니다

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



워크그룹 모드로 전환하려면 모든 도메인 기반 기능을 사용하지 않도록 설정하고 지속적으로 사용 가능한 공유, 새도우 복제본 및 AES를 포함하여 시스템에서 해당 구성을 자동으로 제거해야 합니다. 그러나 "EXAMPLE.COM\userName" 같은 도메인 구성 공유 ACL은 제대로 작동하지 않지만 ONTAP에서는 제거할 수 없습니다. 명령이 완료된 후 외부 툴을 사용하여 가능한 한 빨리 이러한 공유 ACL을 제거합니다. AES가 활성화된 경우 "example.com" 도메인에서 Windows 계정을 비활성화할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 입력하라는 메시지가 표시될 수 있습니다.

- 'vserver cifs modify' 명령의 적절한 매개 변수를 사용하여 다른 속성을 수정합니다.

## 옵션을 사용하여 **SMB** 서버를 사용자 지정합니다

### 사용 가능한 **SMB** 서버 옵션

SMB 서버를 사용자 지정하는 방법을 고려할 때 사용할 수 있는 옵션을 파악하는 것이 유용합니다. 일부 옵션은 SMB 서버에서 일반적으로 사용되지만 일부 옵션은 특정 SMB 기능을 설정하고 구성하는 데 사용됩니다. SMB 서버 옵션은 'vserver cifs options modify' 옵션으로 제어됩니다.

다음 목록은 관리자 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- \* SMB 세션 시간 초과 값 구성 \*

이 옵션을 구성하면 SMB 세션의 연결이 끊기까지의 유휴 시간(초)을 지정할 수 있습니다. 유휴 세션은 사용자가 클라이언트에 열려 있는 파일이나 디렉토리가 없는 세션입니다. 기본값은 900초입니다.

- \* 기본 UNIX 사용자 구성 \*

이 옵션을 구성하면 SMB 서버에서 사용하는 기본 UNIX 사용자를 지정할 수 있습니다. ONTAP은 ""pcuser""(UID 65534)라는 기본 사용자를 자동으로 만들고 ""pcuser""(GID가 65534)라는 그룹을 만든 다음 기본 사용자를 ""pcuser"" 그룹에 추가합니다. SMB 서버를 생성하면 ONTAP는 자동으로 ""pcuser""를 기본 UNIX 사용자로 구성합니다.

- \* 게스트 UNIX 사용자 구성 \*

이 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 매핑될 UNIX 사용자의 이름을 지정할 수 있으므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결할 수 있습니다. 기본적으로 이 옵션은 구성되지 않음(기본값 없음)이므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결하도록 허용하지 않습니다.

- \* 모드 비트에 대한 읽기 권한 실행 활성화 또는 비활성화 \*

이 옵션을 설정하거나 해제하면 UNIX 실행 가능 비트가 설정되지 않은 경우에도 SMB 클라이언트가 읽기 액세스 권한이 있는 UNIX 모드 비트를 사용하여 실행 파일을 실행하도록 허용할지 여부를 지정할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

- \* NFS 클라이언트에서 읽기 전용 파일을 삭제하는 기능을 활성화 또는 비활성화합니다

이 옵션을 설정하거나 해제하면 NFS 클라이언트가 읽기 전용 속성이 설정된 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. NTFS 삭제 의미 체계에서는 읽기 전용 특성이 설정된 경우 파일 또는 폴더를 삭제할 수 없습니다. UNIX 삭제 의미 체계는 읽기 전용 비트를 무시하고 상위 디렉토리 권한을 사용하여 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. 기본 설정은 사용 안 함 으로 NTFS 삭제 의미를 가져옵니다.

- \* Windows 인터넷 이름 서비스 서버 주소 구성 \*

이 옵션을 구성하면 WINS(Windows Internet Name Service) 서버 주소 목록을 심표로 구분된 목록으로 지정할 수 있습니다. IPv4 주소를 지정해야 합니다. IPv6 주소는 지원되지 않습니다. 기본값이 없습니다.

다음 목록은 고급 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- \* CIFS 사용자에게 UNIX 그룹 권한 부여 \*

이 옵션을 구성하면 파일 소유자가 아닌 수신 CIFS 사용자에게 그룹 권한을 부여할 수 있는지 여부를 결정합니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수를 "true"로 설정하면 해당 파일에 대한 그룹 권한이 부여됩니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수가 "false"로 설정된 경우 일반 UNIX 규칙을 적용하여 파일 권한을 부여할 수 있습니다. 이 매개 변수는 권한이 '모드 비트'로 설정되어 있고 NTFS 또는 NFSv4 보안 모드가 있는 파일에는 적용되지 않는 UNIX 보안 스타일 파일에 적용됩니다. 기본 설정은 false입니다.

- \* SMB 1.0 \* 활성화 또는 비활성화

SMB 1.0은 ONTAP 9.3에서 SMB 서버가 생성된 SVM에서 기본적으로 비활성화되어 있습니다.



ONTAP 9.3부터는 ONTAP 9.3에서 생성된 새 SMB 서버에 대해 SMB 1.0이 기본적으로 사용되지 않습니다. 보안 및 규정 준수 향상을 준비하기 위해 가능한 한 빨리 최신 SMB 버전으로 마이그레이션해야 합니다. 자세한 내용은 NetApp 담당자에게 문의하십시오.

- \* SMB 2.x \* 활성화 또는 비활성화

SMB 2.0은 LIF 페일오버를 지원하는 최소 SMB 버전입니다. SMB 2.x를 비활성화하면 ONTAP도 자동으로 SMB 3.X를 비활성화합니다

SMB 2.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- \* SMB 3.0 \* 활성화 또는 비활성화

SMB 3.0은 지속적으로 사용 가능한 공유를 지원하는 최소 SMB 버전입니다. Windows Server 2012 및 Windows 8은 SMB 3.0을 지원하는 최소 Windows 버전입니다.

SMB 3.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- \* SMB 3.1 \* 활성화 또는 비활성화

Windows 10은 SMB 3.1을 지원하는 유일한 Windows 버전입니다.

SMB 3.1은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- \* ODX 복사 오프로드 설정 또는 해제 \*

ODX 복사 오프로드는 Windows 클라이언트에서 지원하는 데 자동으로 사용됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- \* ODX 복사 오프로드에 대한 직접 복사 메커니즘 설정 또는 해제 \*

직접 복사 메커니즘은 Windows 클라이언트가 복사 진행 중에 파일이 변경되지 않도록 하는 모드에서 복사본의 소스 파일을 열려고 할 때 복제 오프로드 작업의 성능을 향상시킵니다. 기본적으로 직접 복사 메커니즘은 활성화되어 있습니다.

- \* 자동 노드 참조 활성화 또는 비활성화 \*

SMB 서버는 자동 노드 조회를 통해 요청된 공유를 통해 액세스한 데이터를 호스팅하는 노드에 대한 데이터 LIF 로컬 클라이언트를 자동으로 참조합니다.

- \* SMB\*에 대한 내보내기 정책 활성화 또는 비활성화

이 옵션은 기본적으로 비활성화되어 있습니다.

- \* 교차점을 재분석 지점으로 사용하여 활성화 또는 비활성화 \*

이 옵션을 활성화하면 SMB 서버는 재분석 지점으로 SMB 클라이언트에 연결 지점을 노출합니다. 이 옵션은 SMB 2.x 또는 SMB 3.0 연결에만 유효합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 옵션은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- \* TCP 연결당 최대 동시 작업 수 구성 \*

기본값은 255입니다.

- \* 로컬 Windows 사용자 및 그룹 기능 활성화 또는 비활성화 \*

이 옵션은 기본적으로 활성화되어 있습니다.

- \* 로컬 Windows 사용자 인증 활성화 또는 비활성화 \*

이 옵션은 기본적으로 활성화되어 있습니다.

- \* VSS 새도우 복제본 기능 활성화 또는 비활성화 \*

ONTAP는 새도우 복제본 기능을 사용하여 SMB를 통한 Hyper-V 솔루션을 사용하여 저장된 데이터의 원격 백업을 수행합니다.

이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- \* 새도 복사본 디렉토리 수준 구성 \*

이 옵션을 구성하면 새도우 복제본 기능을 사용할 때 새도우 복제본을 생성할 디렉토리의 최대 깊이를 정의할 수 있습니다.

이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- \* 이름 매핑에 대한 다중 도메인 검색 기능을 활성화 또는 비활성화합니다 \*

활성화된 경우, UNIX 사용자가 Windows 사용자 이름의 도메인 부분에서 와일드카드(\*)를 사용하여 Windows 도메인 사용자에게 매핑되면(예: \*\\Joe) ONTAP는 양방향 트러스트가 있는 모든 도메인에서 홈 도메인으로 지정된 사용자를 검색합니다. 홈 도메인은 SMB 서버의 컴퓨터 계정이 포함된 도메인입니다.

양방향으로 신뢰할 수 있는 모든 도메인을 검색하는 대신 선호하는 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다. 이 옵션을 사용하도록 설정하고 기본 설정 목록을 구성하면 다중 도메인 이름 매핑 검색을 수행하는 데 기본 설정 목록이 사용됩니다.

기본값은 다중 도메인 이름 매핑 검색을 사용하는 것입니다.

- \* 파일 시스템 섹터 크기 구성 \*

이 옵션을 구성하면 ONTAP에서 SMB 클라이언트에 보고하는 파일 시스템 섹터 크기를 바이트 단위로 구성할 수 있습니다. 이 옵션에는 4096과 512의 두 가지 유효한 값이 있습니다. 기본값은 4096입니다. Windows 응용 프로그램이 512바이트의 섹터 크기만 지원하는 경우 이 값을 '512'로 설정해야 할 수 있습니다.

- \* 동적 액세스 제어 활성화 또는 비활성화 \*

이 옵션을 활성화하면 DAC(Dynamic Access Control)를 사용하여 중앙 액세스 정책을 스테이징하고 그룹 정책 개체를 사용하여 중앙 액세스 정책을 구현하는 등 SMB 서버의 개체를 보호할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

이 옵션은 SVM에서만 지원됩니다.

- \* 인증되지 않은 세션에 대한 액세스 제한 설정(익명 제한) \*

이 옵션을 설정하면 인증되지 않은 세션에 대한 액세스 제한이 결정됩니다. 제한 사항은 익명 사용자에게 적용됩니다. 기본적으로 익명 사용자에게 대한 액세스 제한은 없습니다.

- \* UNIX 효과적인 보안(UNIX 보안 스타일 볼륨 또는 UNIX 효과적인 보안이 포함된 혼합 보안 스타일 볼륨)이 있는 볼륨에서 NTFS ACL 표시를 활성화 또는 비활성화합니다. \*

이 옵션을 설정하거나 해제하면 UNIX 보안이 있는 파일 및 폴더의 파일 보안이 SMB 클라이언트에 제공되는 방식이 결정됩니다. 이 옵션을 설정하면 ONTAP는 UNIX 보안 기능이 있는 볼륨의 파일 및 폴더를 NTFS ACL을 사용한 NTFS 파일 보안으로 SMB 클라이언트에 제공합니다. 사용하지 않도록 설정하면 ONTAP는 UNIX 보안이 설정된 볼륨을 파일 보안 없이 FAT 볼륨으로 제공합니다. 기본적으로 볼륨은 NTFS ACL을 사용한 NTFS 파일 보안을 갖는 것으로 표시됩니다.

- \* SMB 가짜 열기 기능 활성화 또는 비활성화 \*

이 기능을 사용하면 파일 및 디렉토리에 대한 속성 정보를 쿼리할 때 ONTAP에서 열기 및 닫기 요청을 수행하는 방식을 최적화하여 SMB 2.x 및 SMB 3.0 성능을 향상시킬 수 있습니다. 기본적으로 SMB 가짜 열기 기능이 활성화됩니다. 이 옵션은 SMB 2.x 이상에서 만들어진 연결에만 유용합니다.

- \* UNIX 확장 활성화 또는 비활성화 \*

이 옵션을 활성화하면 SMB 서버에서 UNIX 확장이 활성화됩니다. UNIX 확장을 사용하면 POSIX/UNIX 스타일 보안을 SMB 프로토콜을 통해 표시할 수 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

Mac OSX 클라이언트와 같은 UNIX 기반 SMB 클라이언트가 있는 경우 UNIX 확장을 활성화해야 합니다. UNIX 확장을 사용하면 SMB 서버가 POSIX/UNIX 보안 정보를 SMB를 통해 UNIX 기반 클라이언트로 전송한 다음 보안 정보를 POSIX/UNIX 보안으로 변환합니다.

- \* 간단한 이름 검색 지원 활성화 또는 비활성화 \*

이 옵션을 활성화하면 SMB 서버가 짧은 이름으로 검색을 수행할 수 있습니다. 이 옵션을 사용하는 검색 쿼리는 8.3 파일 이름과 긴 파일 이름을 일치시키려고 합니다. 이 파라미터의 기본값은 'false'입니다.

- \* DFS 기능 자동 보급에 대한 지원 활성화 또는 비활성화 \*

이 옵션을 활성화 또는 비활성화하면 SMB 서버가 공유에 연결하는 SMB 2.x 및 SMB 3.0 클라이언트에 DFS 기능을 자동으로 보급할지 여부를 결정합니다. ONTAP는 SMB 액세스를 위한 심볼 링크 구현에 DFS 조회를 사용합니다. 활성화된 경우 SMB 서버는 심볼 링크 액세스가 설정되었는지 여부에 관계없이 항상 DFS 기능을 알립니다. 비활성화된 경우 SMB 서버는 클라이언트가 심볼 링크 액세스가 설정된 공유에 연결할 때만 DFS 기능을 알립니다.

• \* 최대 SMB 크레딧 수 구성 \*

ONTAP 9.4부터, '-max-credits' 옵션을 구성하면 클라이언트와 서버가 SMB 버전 2 이상을 실행하는 경우 SMB 연결에 부여할 크레딧 수를 제한할 수 있습니다. 기본값은 128입니다.

• \* SMB 멀티 채널 \* 에 대한 지원 활성화 또는 비활성화

ONTAP 9.4 이상 릴리스에서 '-is-multichannel-enabled' 옵션을 활성화하면 SMB 서버는 클러스터와 해당 클라이언트에 적절한 NIC가 구축될 때 단일 SMB 세션에 대해 여러 개의 연결을 설정할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다. 이 파라미터의 기본값은 'false'입니다.

SMB 멀티 채널이 활성화되면 다음 매개 변수도 지정할 수 있습니다.

- 다중 채널 세션당 허용되는 최대 연결 수입니다. 이 매개 변수의 기본값은 32입니다.
- Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 이 매개 변수의 기본값은 256입니다.

## SMB 서버 옵션 구성

SVM(스토리지 가상 시스템)에서 SMB 서버를 생성한 후에는 언제든지 SMB 서버 옵션을 구성할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

SMB 서버 옵션을 구성하려면...	명령 입력...
관리 권한 수준에서 설정합니다	'vserver cifs options modify -vserver_vserver_name options_'
고급 권한 수준에서 설정합니다	a. 세트 프리빌리지 고급 b. 'vserver cifs options modify -vserver_vserver_name options_' c. 'Set-Privilege admin'입니다

SMB 서버 옵션 구성에 대한 자세한 내용은 'vserver cifs options modify' 명령의 man 페이지를 참조하십시오.

## SMB 사용자에게 UNIX 그룹 권한 부여 를 구성합니다

들어오는 SMB 사용자가 파일 소유자가 아닌 경우에도 파일 또는 디렉토리에 액세스할 수 있는 그룹 권한을 부여하도록 이 옵션을 구성할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX 그룹 권한 부여를 적절히 구성합니다.



원하는 경우	명령을 입력합니다
사용자가 파일 소유자가 아니더라도 파일 또는 디렉토리에 대한 액세스를 활성화하여 그룹 권한을 얻습니다	'vserver cifs options modify --grant-unix-group-perms-to-others true'
파일 또는 디렉토리에 대한 액세스를 비활성화하여 사용자가 파일 소유자가 아니더라도 그룹 권한을 얻습니다	'vserver cifs options modify --grant-unix-group-perms-to-others false'

3. 이 옵션이 원하는 값으로 설정되어 있는지 확인합니다. 'vserver cifs options show --fields grant-unix-group-perms-to-others'

4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

익명 사용자의 액세스 제한을 구성합니다

기본적으로 인증되지 않은 익명 사용자(*null user* 라고도 함)는 네트워크의 특정 정보에 액세스할 수 있습니다. SMB 서버 옵션을 사용하여 익명 사용자의 액세스 제한을 구성할 수 있습니다.

이 작업에 대해

익명 제한 SMB 서버 옵션은 Windows의 RestrictAnonymous 레지스트리 항목에 해당합니다.

익명 사용자는 사용자 이름 및 세부 정보, 계정 정책 및 공유 이름을 포함하여 네트워크의 Windows 호스트에서 특정 유형의 시스템 정보를 나열하거나 열거할 수 있습니다. 다음 세 가지 액세스 제한 설정 중 하나를 지정하여 익명 사용자에게 대한 액세스를 제어할 수 있습니다.

값	설명
무제한(기본값)	익명 사용자에게 대한 액세스 제한을 지정하지 않습니다.
번호 매기기	익명 사용자에게 대해서만 열거를 제한하도록 지정합니다.
"접근 불가"	익명 사용자에게 대한 액세스가 제한되도록 지정합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 익명 제한 설정: 'vserver cifs options modify -vserver\_vserver\_name\_-restrict-anonymous{no-restriction|no-enumeration|no-access}'를 구성합니다
3. 옵션이 원하는 값('vserver cifs options show -vserver\_vserver\_name\_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

[사용 가능한 SMB 서버 옵션](#)

**UNIX** 보안 스타일 데이터를 위해 **SMB** 클라이언트에 파일 보안을 제공하는 방법을 관리합니다

**UNIX** 보안 스타일 데이터 개요를 위해 **SMB** 클라이언트에 파일 보안을 제공하는 방법을 관리합니다

SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화하여 UNIX 보안 스타일 데이터용 파일 보안을 SMB 클라이언트에 제공하는 방법을 선택할 수 있습니다. 각 설정에는 비즈니스 요구 사항에 가장 적합한 설정을 선택해야 한다는 점을 이해해야 합니다.

기본적으로 ONTAP은 UNIX 보안 스타일 볼륨에 대한 UNIX 권한을 SMB 클라이언트에 NTFS ACL로 제공합니다. 다음과 같이 이 방법이 필요한 시나리오가 있습니다.

- Windows 속성 상자의 \* 보안 \* 탭을 사용하여 UNIX 권한을 보고 편집하려는 경우

UNIX 시스템에서 작업이 허용되지 않는 경우 Windows 클라이언트에서 권한을 수정할 수 없습니다. 예를 들어 UNIX 시스템에서는 이 작업을 허용하지 않으므로 소유하지 않는 파일의 소유권을 변경할 수 없습니다. 이 제한 사항으로 인해 SMB 클라이언트가 파일 및 폴더에 설정된 UNIX 권한을 우회하지 못합니다.

- 사용자는 Microsoft Office와 같은 특정 Windows 응용 프로그램을 사용하여 UNIX 보안 스타일 볼륨에서 파일을 편집 및 저장하고 있습니다. 여기서 ONTAP는 저장 작업 중에 UNIX 권한을 유지해야 합니다.
- 사용자 환경에는 사용 중인 파일에 대해 NTFS ACL을 읽을 것으로 예상되는 특정 Windows 애플리케이션이 있습니다.

경우에 따라 UNIX 사용 권한을 NTFS ACL로 표시하지 않도록 설정할 수 있습니다. 이 기능을 비활성화하면 ONTAP는 UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 제공합니다. UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 표시하는 이유는 다음과 같습니다.

- UNIX 클라이언트에서 마운트를 사용하여 UNIX 사용 권한만 변경할 수 있습니다.

UNIX 보안 스타일 볼륨이 SMB 클라이언트에 매핑된 경우에는 보안 탭을 사용할 수 없습니다. 매핑된 드라이브는 파일 권한이 없는 FAT 파일 시스템으로 포맷된 것 같습니다.

- 액세스 파일 및 폴더에 NTFS ACL을 설정하는 SMB를 통해 애플리케이션을 사용 중이며, UNIX 보안 스타일 볼륨에 데이터가 있는 경우 오류가 발생할 수 있습니다.

ONTAP가 볼륨을 FAT로 보고하는 경우 응용 프로그램은 ACL을 변경하지 않습니다.

## 관련 정보

[FlexVol 볼륨에서 보안 스타일 구성](#)

[Qtree에서 보안 스타일 구성](#)

**UNIX** 보안 스타일 데이터에 대한 **NTFS ACL** 표시를 활성화 또는 비활성화합니다

UNIX 보안 스타일 데이터(UNIX 보안 스타일 볼륨 및 UNIX 효과적인 보안이 포함된 혼합 보안 스타일 볼륨)를 위해 SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화할 수 있습니다.

## 이 작업에 대해

이 옵션을 설정하면 ONTAP는 효율적인 UNIX 보안 스타일을 사용하는 볼륨의 파일 및 폴더를 NTFS ACL을 갖는 것으로 SMB 클라이언트에 제공합니다. 이 옵션을 비활성화하면 볼륨이 SMB 클라이언트에 FAT 볼륨으로 표시됩니다.

기본값은 NTFS ACL을 SMB 클라이언트에 제공하는 것입니다.

#### 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX NTFS ACL 옵션 설정을 구성합니다. 'vserver cifs options modify -vserver\_vserver\_name\_-is-unix-NT -acl-enabled{true|false}'
3. 옵션이 원하는 값('vserver cifs options show -vserver\_vserver\_name\_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

#### ONTAP에서 UNIX 사용 권한을 유지하는 방법

현재 UNIX 사용 권한이 있는 FlexVol 볼륨의 파일을 Windows 응용 프로그램에서 편집하고 저장하면 ONTAP에서 UNIX 사용 권한을 보존할 수 있습니다.

Windows 클라이언트의 응용 프로그램이 파일을 편집하고 저장할 때 파일의 보안 속성을 읽고, 새 임시 파일을 만들고, 해당 속성을 임시 파일에 적용한 다음 임시 파일에 원래 파일 이름을 지정합니다.

Windows 클라이언트가 보안 속성에 대한 쿼리를 수행할 때 UNIX 권한을 정확하게 나타내는 생성된 ACL을 받습니다. 이 생성된 ACL의 유일한 목적은 파일이 Windows 애플리케이션에 의해 업데이트되므로 파일의 UNIX 사용 권한을 보존하여 결과 파일이 동일한 UNIX 사용 권한을 갖도록 하는 것입니다. ONTAP는 생성된 ACL을 사용하여 NTFS ACL을 설정하지 않습니다.

#### Windows 보안 탭을 사용하여 UNIX 사용 권한을 관리합니다

SVM에서 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 대한 UNIX 권한을 조작하려는 경우 Windows 클라이언트의 보안 탭을 사용할 수 있습니다. 또는 Windows ACL을 쿼리하고 설정할 수 있는 응용 프로그램을 사용할 수도 있습니다.

##### • UNIX 사용 권한 수정

Windows 보안 탭을 사용하여 혼합 보안 스타일 볼륨 또는 qtree에 대한 UNIX 권한을 보고 변경할 수 있습니다. 기본 Windows 보안 탭을 사용하여 UNIX 권한을 변경하는 경우 변경하기 전에 먼저 편집할 기존 ACE(모드 비트를 0으로 설정)를 제거해야 합니다. 또는 고급 편집기를 사용하여 권한을 변경할 수도 있습니다.

모드 권한을 사용하는 경우 나열된 UID, GID 및 기타(컴퓨터에 계정이 있는 다른 모든 사용자)에 대한 모드 권한을 직접 변경할 수 있습니다. 예를 들어, 표시된 UID에 r-x 권한이 있는 경우 UID 권한을 rwx로 변경할 수 있습니다.

##### • UNIX 권한을 NTFS 권한으로 변경합니다

Windows 보안 탭을 사용하면 파일 및 폴더에 UNIX 유효 보안 스타일이 있는 혼합 보안 스타일 볼륨 또는 qtree의 UNIX 보안 개체를 Windows 보안 개체로 대체할 수 있습니다.

원하는 Windows 사용자 및 그룹 개체로 대체하려면 먼저 나열된 모든 UNIX 권한 항목을 제거해야 합니다. 그런 다음 Windows 사용자 및 그룹 개체에서 NTFS 기반 ACL을 구성할 수 있습니다. 모든 UNIX 보안 개체를 제거하고 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 Windows 사용자 및 그룹만 추가하면 파일 또는 폴더의 효과적인 보안 스타일이 UNIX에서 NTFS로 변경됩니다.

폴더에 대한 권한을 변경할 때 기본 Windows 동작은 이러한 변경 내용을 모든 하위 폴더 및 파일에 전파하는 것입니다. 따라서 보안 스타일의 변경 사항을 모든 하위 폴더, 하위 폴더 및 파일에 전파하지 않으려면 전파 선택 사항을 원하는 설정으로 변경해야 합니다.

## SMB 서버 보안 설정을 관리합니다

### ONTAP가 SMB 클라이언트 인증을 처리하는 방법

사용자가 SVM에 포함된 데이터에 액세스하기 위해 SMB 연결을 생성하려면 먼저 SMB 서버가 속해 있는 도메인에서 인증을 받아야 합니다. SMB 서버는 Kerberos와 NTLM(NTLMv1 또는 NTLMv2)의 두 가지 인증 방법을 지원합니다. Kerberos는 도메인 사용자를 인증하는 데 사용되는 기본 방법입니다.

#### Kerberos 인증

ONTAP는 인증된 SMB 세션을 생성할 때 Kerberos 인증을 지원합니다.

Kerberos는 Active Directory의 기본 인증 서비스입니다. Kerberos 서버 또는 Kerberos KDC(Key Distribution Center) 서비스는 Active Directory에 보안 원칙에 대한 정보를 저장하고 검색합니다. NTLM 모델과 달리 SMB 서버와 같은 다른 컴퓨터와 세션을 설정하려는 Active Directory 클라이언트는 KDC에 직접 문의하여 세션 자격 증명을 얻습니다.

#### NTLM 인증

NTLM 클라이언트 인증은 암호를 기반으로 사용자별 비밀번호에 대한 공유 지식을 기반으로 하는 본인 확인 응답 프로토콜을 사용하여 수행됩니다.

사용자가 로컬 Windows 사용자 계정을 사용하여 SMB 연결을 만들면 NTLMv2를 사용하여 SMB 서버에서 로컬로 인증이 수행됩니다.

### SVM 재해 복구 구성의 SMB 서버 보안 설정 지침

ID가 보존되지 않는 재해 복구 대상으로 구성된 SVM(SnapMirror 구성에서 'identity-preserve' 옵션이 'false'로 설정됨)을 생성하기 전에 SVM 대상에서 SMB 서버 보안 설정이 관리되는 방식을 알아야 합니다.

- 기본이 아닌 SMB 서버 보안 설정은 대상에 복제되지 않습니다.

대상 SVM에서 SMB 서버를 생성할 때 모든 SMB 서버 보안 설정이 기본값으로 설정됩니다. SVM 재해 복구 대상이 초기화, 업데이트 또는 재동기화되면 소스의 SMB 서버 보안 설정이 타겟으로 복제되지 않습니다.

- 기본이 아닌 SMB 서버 보안 설정을 수동으로 구성해야 합니다.

소스 SVM에 기본값이 아닌 SMB 서버 보안 설정이 구성되어 있는 경우 SnapMirror 관계가 깨진 후, 대상이 읽기-쓰기 상태가 되면 대상 SVM에서 동일한 설정을 수동으로 구성해야 합니다.

### SMB 서버 보안 설정에 대한 정보를 표시합니다

SMB 서버 보안 설정에 대한 정보를 SVM(스토리지 가상 머신)에 표시할 수 있습니다. 이 정보를 사용하여 보안 설정이 올바른지 확인할 수 있습니다.

#### 이 작업에 대해

표시된 보안 설정은 해당 개체의 기본값이거나 ONTAP CLI를 사용하거나 Active Directory 그룹 정책 개체(GPO)를 사용하여 구성된 기본값이 아닌 값일 수 있습니다.

일부 옵션이 유효하지 않으므로 워크그룹 모드에서 SMB 서버에 대해 "vserver cifs security show" 명령을 사용하지 마십시오.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 모든 보안 설정	'vserver cifs security show -vserver_vserver_name_'
SVM의 특정 보안 설정 또는 설정	'vserver cifs security show -vserver_vserver_name_ - 필드 [fieldname,...]'를 입력하면 '-fields?'를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

예

다음 예는 SVM VS1 보안 설정을 모두 보여줍니다.

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

Vserver: vs1

Kerberos Clock Skew:          5 minutes
Kerberos Ticket Age:         10 hours
Kerberos Renewal Age:        7 days
Kerberos KDC Timeout:        3 seconds
Is Signing Required:         false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled:    false
LM Compatibility Level:       lm-ntlm-ntlmv2-krb
Is SMB Encryption Required:    false
Client Session Security:      none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

표시되는 설정은 실행 중인 ONTAP 버전에 따라 다릅니다.

다음 예에서는 SVM VS1 Kerberos 클록 편종을 보여 줍니다.

```
cluster1::> vsriver cifs security show -vsriver vs1 -fields kerberos-
clock-skew
```

```
vsriver kerberos-clock-skew
-----
vs1      5
```

관련 정보

[GPO 구성에 대한 정보 표시](#)

로컬 **SMB** 사용자에게 대해 필요한 암호 복잡성을 설정하거나 해제합니다

필수 비밀번호 복잡성은 스토리지 가상 시스템(SVM)의 로컬 SMB 사용자를 위해 향상된 보안을 제공합니다. 필요한 암호 복잡성 기능은 기본적으로 활성화되어 있습니다. 이 기능을 사용하지 않도록 설정하고 언제든지 다시 사용하도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버에서 로컬 사용자, 로컬 그룹 및 로컬 사용자 인증을 설정해야 합니다.



이 작업에 대해

일부 옵션이 유효하지 않으므로 워크그룹 모드에서 CIFS 서버에 대해 "vsriver cifs security modify" 명령을 사용하면 안 됩니다.

단계

1. 다음 작업 중 하나를 수행합니다.

로컬 <b>SMB</b> 사용자에게 대한 암호 복잡성에 필요한 경우...	명령 입력...
활성화됨	'vsriver cifs security modify -vsriver_vsriver_name_-is-password-Complexity -required true'
사용 안 함	'vsriver cifs security modify -vsriver_vsriver_name_-is-password-Complexity -required false'

2. 필요한 암호 복잡성에 대한 보안 설정을 확인합니다. 'vsriver cifs security show -vsriver\_vsriver\_name\_'

예

다음 예에서는 SVM VS1 용 로컬 SMB 사용자에게 대해 필요한 암호 복잡성이 활성화된 것을 보여 줍니다.

```
cluster1::> vsriver cifs security modify -vsriver vs1 -is-password
-complexity-required true

cluster1::> vsriver cifs security show -vsriver vs1 -fields is-password-
complexity-required
vsriver is-password-complexity-required
-----
vs1      true
```

## 관련 정보

[CIFS 서버 보안 설정에 대한 정보를 표시합니다](#)

[로컬 사용자 및 그룹을 인증 및 인증에 사용합니다](#)

[로컬 사용자 암호 요구 사항](#)

[로컬 사용자 계정 암호 변경](#)

## CIFS 서버 Kerberos 보안 설정을 수정합니다

허용되는 최대 Kerberos 클럭 비뚤어짐 시간, Kerberos 티켓 수명 및 티켓 갱신 최대 일 수를 비롯한 특정 CIFS 서버 Kerberos 보안 설정을 수정할 수 있습니다.

### 이 작업에 대해

'vsriver cifs security modify' 명령을 사용하여 CIFS 서버 Kerberos 설정을 수정하면 '-vsriver' 매개 변수로 지정한 단일 SVM(스토리지 가상 머신)에서만 설정이 수정됩니다. Active Directory 그룹 정책 개체(GPO)를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM에 대한 Kerberos 보안 설정을 중앙에서 관리할 수 있습니다.

### 단계

1. 다음 작업 중 하나 이상을 수행합니다.

원하는 작업	입력...
허용되는 최대 Kerberos 클럭 편중 시간을 분(9.13.1 이상) 또는 초(9.12.1 이하)로 지정합니다.	'vsriver cifs security modify -vsriver_vserver_name_-Kerberos-clock -suts_integer_in_minutes_'  기본 설정은 5분입니다.
Kerberos 티켓 수명(시간)을 지정합니다.	'vsriver cifs security modify -vsriver_vserver_name_-Kerberos-티켓-age integer_in_hours'를 선택합니다  기본 설정은 10시간입니다.

티켓 갱신 최대 일 수를 지정하십시오.	'vserver cifs security modify - vserver_vserver_name_ - Kerberos - renew - age_integer_in_days _'  기본 설정은 7일입니다.
모든 KDC가 도달할 수 없음으로 표시되는 KDC의 소켓에 대한 시간 제한을 지정합니다.	'vserver cifs security modify -vserver_vserver_name_-Kerberos-KDC -timeout_integer_in_seconds _'  기본 설정은 3초입니다.

## 2. Kerberos 보안 설정을 확인합니다.

'vserver cifs security show -vserver\_vserver\_name\_'

예

다음 예에서는 Kerberos 보안을 다음과 같이 변경합니다. ""Kerberos Clock Skew""는 3분으로 설정되고 ""Kerberos Ticket Age""는 SVM VS1 v1의 경우 8시간으로 설정됩니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew: 3 minutes
Kerberos Ticket Age: 8 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
```

## 관련 정보

["CIFS 서버 보안 설정에 대한 정보를 표시합니다"](#)

["지원되는 GPO"](#)

["CIFS 서버에 그룹 정책 객체 적용"](#)



## SMB 서버 최소 인증 보안 수준을 설정합니다

SMB 클라이언트 액세스에 대한 비즈니스 보안 요구 사항을 충족하도록 SMB 서버에서 `_LMCompatibilityLevel_`이라고도 하는 SMB 서버 최소 보안 수준을 설정할 수 있습니다. 최소 보안 수준은 SMB 서버가 SMB 클라이언트에서 허용하는 최소 보안 토큰입니다.



이 작업에 대해

- 워크그룹 모드의 SMB 서버는 NTLM 인증만 지원합니다. Kerberos 인증은 지원되지 않습니다.
- LMCompatibilityLevel 관리자 인증이 아닌 SMB 클라이언트 인증에만 적용됩니다.

최소 인증 보안 수준을 지원되는 네 가지 보안 수준 중 하나로 설정할 수 있습니다.

값	설명
lm-NTLM-NTLMv2-KRB(기본값)	SVM(스토리지 가상 시스템)은 LM, NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다.
NTLM-NTLMv2-KRB	SVM은 NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 인증을 거부합니다.
NTLMv2-KRB	SVM은 NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 및 NTLM 인증을 거부합니다.
KRB	SVM은 Kerberos 인증 보안만 수락합니다. SVM은 LM, NTLM 및 NTLMv2 인증을 거부합니다.

### 단계

1. 최소 인증 보안 수준을 설정합니다. 'vserver cifs security modify -vserver\_vserver\_name\_-lm -compatibility -level{lm-NTLM-NTLMv2-KRB | NTLM-NTLMv2-KRB | NTLMv2-KRB | KRB | KRB}'
2. 인증 보안 수준이 원하는 수준('vserver cifs security show -vserver\_vserver\_name\_')으로 설정되어 있는지 확인합니다

### 관련 정보

[Kerberos 기반 통신을 위한 AES 암호화 활성화 또는 비활성화](#)

**AES** 암호화를 사용하여 **Kerberos** 기반 통신을 위한 강력한 보안을 구성합니다

Kerberos 기반 통신을 사용하여 보안을 강화하기 위해 SMB 서버에서 AES-256 및 AES-128 암호화를 활성화할 수 있습니다. 기본적으로 SVM에서 SMB 서버를 생성할 때 AES(고급 암호화 표준) 암호화가 사용되지 않습니다. AES 암호화로 제공되는 강력한 보안을 활용하려면 이 기능을 활성화해야 합니다.

SMB를 위한 Kerberos 관련 통신은 SVM에서 SMB 서버를 생성하는 동안이나 SMB 세션 설정 단계에서 사용됩니다. SMB 서버는 Kerberos 통신을 위해 다음과 같은 암호화 유형을 지원합니다.

- AES 256

- AES 128
- DES
- RC4-HMAC

Kerberos 통신에 가장 높은 보안 암호화 유형을 사용하려면 SVM에서 Kerberos 통신에 AES 암호화를 사용하도록 설정해야 합니다.

SMB 서버가 생성되면 도메인 컨트롤러는 Active Directory에 컴퓨터 시스템 계정을 만듭니다. 이때 KDC는 특정 컴퓨터 계정의 암호화 기능을 인식합니다. 그런 다음 인증 중에 클라이언트가 서버에 제공하는 서비스 티켓을 암호화하기 위해 특정 암호화 유형을 선택합니다.

ONTAP 9.12.1부터 Active Directory(AD) KDC에 알릴 암호화 유형을 지정할 수 있습니다. 를 사용할 수 있습니다 `-advertised-enc-types` 권장 암호화 유형을 활성화하는 옵션으로, 약한 암호화 유형을 비활성화하는 데 사용할 수 있습니다. 자세한 내용을 알아보십시오 ["Kerberos 기반 통신을 위한 암호화 유형을 활성화 및 비활성화합니다"](#).



인텔 AES 새 명령어(인텔 AES NI)는 SMB 3.0에서 사용할 수 있으며, AES 알고리즘을 개선하고 지원되는 프로세서 제품군에서 데이터 암호화를 가속화합니다. SMB 3.1.1부터 AES-128-GCM은 SMB 암호화에 사용되는 해시 알고리즘으로 AES-128-CCM을 대체합니다.

관련 정보

[CIFS 서버 Kerberos 보안 설정을 수정합니다](#)

**Kerberos** 기반 통신을 위해 **AES** 암호화를 사용하거나 사용하지 않도록 설정합니다

Kerberos 기반 통신에서 가장 강력한 보안을 활용하려면 SMB 서버에서 AES-256 및 AES-128 암호화를 사용해야 합니다. ONTAP 9.13.1부터 AES 암호화는 기본적으로 사용하도록 설정됩니다. SMB 서버가 AD(Active Directory) KDC와 Kerberos 기반 통신을 위해 AES 암호화 유형을 선택하지 않도록 하려면 AES 암호화를 사용하지 않도록 설정할 수 있습니다.

AES 암호화가 기본적으로 사용되는지 여부와 암호화 유형을 지정하는 옵션이 있는지 여부는 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	AES 암호화 사용...	암호화 유형을 지정할 수 있습니까?
9.13.1 이상	기본적으로 사용됩니다	예
9.12.1	수동	예
9.11.1 이하	수동	아니요

ONTAP 9.12.1부터 AES 암호화는 을 사용하여 활성화 및 비활성화됩니다 `-advertised-enc-types` 옵션: AD KDC에 보급된 암호화 유형을 지정할 수 있습니다. 기본 설정은 입니다 `rc4` 및 `des` 그러나 AES 유형이 지정되면 AES 암호화가 활성화됩니다. 이 옵션을 사용하여 약한 RC4 및 DES 암호화 유형을 명시적으로 비활성화할 수도 있습니다. ONTAP 9.11.1 이하 버전에서는 을 사용해야 합니다 `-is-aes-encryption-enabled` AES 암호화를 활성화 및 비활성화하는 옵션과 암호화 유형을 지정할 수 없습니다.

보안을 강화하기 위해 SVM(Storage Virtual Machine)은 AES 보안 옵션을 수정할 때마다 AD에서 시스템 계정 암호를 변경합니다. 암호를 변경하려면 컴퓨터 계정이 포함된 OU(조직 구성 단위)에 대한 관리 AD 자격 증명이 필요할 수 있습니다.

SVM이 ID가 보존되지 않는 재해 복구 대상으로 구성된 경우( `-identity-preserve` 옵션이 로 설정되어 있습니다

`false` SnapMirror 구성에서 기본 SMB 서버가 아닌 보안 설정은 대상에 복제되지 않습니다. 소스 SVM에서 AES 암호화를 사용하도록 설정한 경우 수동으로 활성화해야 합니다.

## 예 1. 단계

### ONTAP 9.12.1 이상

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 AES 암호화 유형을 원하는 경우...	명령 입력...
활성화됨	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
사용 안 함	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

◦ 참고: \* -is-aes-encryption-enabled 옵션은 ONTAP 9.12.1에서 사용되지 않으며 이후 릴리스에서 제거될 수 있습니다.

2. AES 암호화가 필요에 따라 활성화 또는 비활성화되었는지 확인합니다. `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

### 예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc  
-types aes-128,aes-256  
  
cluster1::> vserver cifs security show -vserver vs1 -fields advertised-  
enc-types  
  
vserver   advertised-enc-types  
-----  
vs1       aes-128,aes-256
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vsserver cifs security modify -vsserver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsserver cifs security show -vsserver vs2 -fields advertised-
enc-types
```

```
vsserver  advertised-enc-types
-----  -
vs2       aes-128,aes-256
```

#### ONTAP 9.11.1 이전 버전

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 AES 암호화 유형을 원하는 경우...	명령 입력...
활성화됨	'vsserver cifs security modify -vsserver vsserver_name -is-aes-encryption-enabled true'
사용 안 함	'vsserver cifs security modify -vsserver vsserver_name -is-aes-encryption-enabled false'

2. AES 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vsserver cifs security show -vsserver vsserver\_name -fields is -aes-encryption-enabled'

AES 암호화가 활성화된 경우 is-aes-encryption-enabled 필드가 true로 표시되고, 비활성화된 경우 false로 표시됩니다.

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vsriver cifs security modify -vsriver vs1 -is-aes
-encryption-enabled true

cluster1::> vsriver cifs security show -vsriver vs1 -fields is-aes-
encryption-enabled

vsriver  is-aes-encryption-enabled
-----
vs1      true
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vsriver cifs security modify -vsriver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vsriver cifs security show -vsriver vs2 -fields is-aes-
encryption-enabled

vsriver  is-aes-encryption-enabled
-----
vs2      true
```

**SMB** 서명을 사용하여 네트워크 보안을 강화합니다

**SMB** 서명을 사용하여 네트워크 보안 개요를 개선합니다

SMB 서명을 사용하면 SMB 서버와 클라이언트 사이의 네트워크 트래픽이 손상되지 않도록 할 수 있으며, 재생 공격을 차단하여 이 작업을 수행합니다. 기본적으로 ONTAP는 클라이언트가 요청할 때 SMB 서명을 지원합니다. 필요에 따라 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버를 구성할 수 있습니다.

**SMB** 서명 정책이 **CIFS** 서버와의 통신에 미치는 영향

CIFS 서버 SMB 서명 보안 설정 외에도 Windows 클라이언트의 두 SMB 서명 정책은

클라이언트와 CIFS 서버 간의 디지털 서명을 제어합니다. 비즈니스 요구 사항에 맞게 설정을 구성할 수 있습니다.

클라이언트 SMB 정책은 MMC(Microsoft Management Console) 또는 Active Directory GPO를 사용하여 구성되는 Windows 로컬 보안 정책 설정을 통해 제어됩니다. 클라이언트 SMB 서명 및 보안 문제에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

다음은 Microsoft 클라이언트에 대한 두 가지 SMB 서명 정책에 대한 설명입니다.

- 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)'

이 설정은 클라이언트의 SMB 서명 기능이 설정되었는지 여부를 제어합니다. 기본적으로 활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 CIFS 서버와의 클라이언트 통신은 CIFS 서버의 SMB 서명 설정에 따라 달라집니다.

- 마이크로네트워크 클라이언트: 디지털 서명 통신(항상)

이 설정은 클라이언트가 서버와 통신하기 위해 SMB 서명을 필요로 하는지 제어합니다. 기본적으로 비활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 SMB 서명 동작은 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)' 및 CIFS 서버의 설정에 대한 정책 설정을 기반으로 합니다.



환경에 SMB 서명이 필요하도록 구성된 Windows 클라이언트가 포함된 경우 CIFS 서버에서 SMB 서명을 설정해야 합니다. 그렇지 않으면 CIFS 서버가 이러한 시스템에 데이터를 제공할 수 없습니다.

클라이언트 및 CIFS 서버 SMB 서명 설정의 효과적인 결과는 SMB 세션이 SMB 1.0 또는 SMB 2.x 이상을 사용하는지 여부에 따라 달라집니다.

다음 표에는 세션이 SMB 1.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.

클라이언트	ONTAP — 서명이 필요하지 않습니다	ONTAP — 서명이 필요합니다
서명이 비활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 비활성화되었으며 필수입니다	서명됨	서명됨
서명이 설정되어 있어야 합니다	서명됨	서명됨



클라이언트에서 서명이 비활성화되었지만 CIFS 서버에서 필요한 경우 이전 Windows SMB 1 클라이언트와 일부 비 Windows SMB 1 클라이언트가 연결되지 않을 수 있습니다.

다음 표에는 세션에서 SMB 2.x 또는 SMB 3.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.



SMB 2.x 및 SMB 3.0 클라이언트의 경우 SMB 서명이 항상 사용하도록 설정됩니다. 비활성화할 수 없습니다.

클라이언트	ONTAP — 서명이 필요하지 않습니다	ONTAP — 서명이 필요합니다
서명이 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 필요합니다	서명됨	서명됨

다음 표에는 기본 Microsoft 클라이언트 및 서버 SMB 서명 동작이 요약되어 있습니다.

프로토콜	해시 알고리즘입니다	활성화/비활성화할 수 있습니다	필요/필요하지 않습니다	클라이언트 기본값입니다	서버 기본값	DC 기본값
SMB 1.0	MD5	예	예	활성화됨(필요하지 않음)	사용 안 함(필수 아님)	필수 요소입니다
SMB 2.x	HMAC SHA-256	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다
SMB 3.0	AES-CMAC	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다



Microsoft는 더 이상 '고유 서명 통신(클라이언트에서 동의한 경우)' 또는 '고유 서명 통신(서버에서 동의한 경우)' 그룹 정책 설정을 사용할 것을 권장하지 않습니다. Microsoft는 또한 "EnableSecuritySignature" 레지스트리 설정을 더 이상 사용하지 않을 것을 권장합니다. 이러한 옵션은 SMB 1 동작에만 영향을 미치며 Digitally sign communications (Always)(항상 서명 통신) 그룹 정책 설정 또는 RequireSecuritySignature(요구 보안 서명) 레지스트리 설정으로 대체할 수 있습니다. 또한 Microsoft 블로그에서 자세한 정보를 얻을 수 있습니다. [The SMB 서명의 기본 사항\(SMB1 및 SMB2 모두 포함\)](#)

#### SMB 서명의 성능 영향

SMB 세션에서 SMB 서명을 사용하면 Windows 클라이언트와 주고 받는 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드) 모두에 영향을 미칩니다.

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 서명된 SMB 트래픽의 성능을 향상시킬 수 있습니다. SMB 서명 오프로드는 SMB 서명이 설정된 경우 기본적으로 설정됩니다.

향상된 SMB 서명 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 서명의 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경에서 테스트를 통해서만 확인할 수 있습니다.



대부분의 Windows 클라이언트는 서버에서 SMB 서명을 사용하는 경우 기본적으로 협상합니다. 일부 Windows 클라이언트에 대해 SMB 보호가 필요하고 SMB 서명으로 인해 성능 문제가 발생하는 경우 재생 공격에 대한 보호가 필요하지 않은 Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정할 수 있습니다. Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

**SMB** 서명 구성을 위한 권장 사항입니다

SMB 클라이언트와 CIFS 서버 간에 SMB 서명 동작을 구성하여 보안 요구 사항을 충족할 수 있습니다. CIFS 서버에서 SMB 서명을 구성할 때 선택하는 설정은 보안 요구 사항에 따라 다릅니다.

클라이언트 또는 CIFS 서버에서 SMB 서명을 구성할 수 있습니다. SMB 서명을 구성할 때 다음 권장 사항을 고려하십시오.

만약...	권장 사항...
클라이언트와 서버 간의 통신 보안을 강화하려는 경우	클라이언트에서 'Require Option(Sign Always)' 보안 설정을 활성화하여 클라이언트에서 SMB 서명이 필요하도록 합니다.
모든 SMB 트래픽이 특정 SVM(스토리지 가상 머신)에 서명하기를 원합니다	SMB 서명이 필요하도록 보안 설정을 구성하여 CIFS 서버에 SMB 서명이 필요합니다.

Windows 클라이언트 보안 설정 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

여러 데이터 LIF가 구성된 경우 **SMB** 서명을 위한 지침입니다

SMB 서버에서 필요한 SMB 서명을 설정하거나 해제하는 경우 SVM에 대한 여러 데이터 LIF 구성에 대한 지침을 숙지해야 합니다.

SMB 서버를 구성할 때 여러 데이터 LIF가 구성되어 있을 수 있습니다. 이 경우 DNS 서버에 동일한 SMB 서버 호스트 이름을 사용하는 CIFS 서버에 대한 여러 개의 "A" 레코드 항목이 포함되어 있고 각 항목은 고유한 IP 주소를 사용합니다. 예를 들어, 두 개의 데이터 LIF가 구성된 SMB 서버의 DNS 'A' 레코드 항목은 다음과 같습니다.

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

일반적으로 필요한 SMB 서명 설정을 변경하면 클라이언트의 새 연결만 SMB 서명 설정의 변경 사항에 영향을 받습니다. 그러나 이 동작에 대한 예외는 있습니다. 클라이언트가 공유에 대한 기존 연결을 가지고 있고, 원래 연결을 유지하면서 설정을 변경한 후 클라이언트가 동일한 공유에 대한 새 연결을 생성하는 경우가 있습니다. 이 경우 새로운 SMB 연결과 기존 SMB 연결이 모두 새로운 SMB 서명 요구 사항을 적용합니다.

다음 예제를 고려해 보십시오.

1. CLIENT1은 'O:\' 경로를 사용하여 SMB 서명이 필요 없이 공유에 연결합니다.
2. 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버 구성을 수정합니다.
3. CLIENT1은 '\:' 경로를 사용하여('O:\' 경로를 사용하여 연결을 유지하면서) 필요한 SMB 서명과 동일한 공유에 연결합니다.

4. 그 결과, "O:\\"와 "s:\\" 드라이브 모두에서 데이터에 액세스할 때 SMB 서명이 사용됩니다.

수신 **SMB** 트래픽에 필요한 **SMB** 서명을 설정하거나 해제합니다

필요한 SMB 서명을 설정하여 클라이언트가 SMB 메시지에 서명하도록 요구 사항을 적용할 수 있습니다. 활성화된 경우 ONTAP은 유효한 서명이 있는 경우에만 SMB 메시지를 수락합니다. SMB 서명을 허용하되 SMB 서명이 필요하지 않은 경우 필요한 SMB 서명을 사용하지 않도록 설정할 수 있습니다.

이 작업에 대해

기본적으로 필요한 SMB 서명은 사용되지 않습니다. 필요한 SMB 서명을 언제든지 설정하거나 해제할 수 있습니다.

다음과 같은 상황에서는 SMB 서명이 기본적으로 비활성화되어 있지 않습니다.



1. 필요한 SMB 서명이 설정되어 있고 클러스터가 SMB 서명을 지원하지 않는 ONTAP 버전으로 되돌려집니다.
2. 이후 클러스터는 SMB 서명을 지원하는 ONTAP 버전으로 업그레이드됩니다.

이러한 경우 지원되는 ONTAP 버전에 원래 구성된 SMB 서명 구성은 재버전과 후속 업그레이드를 통해 유지됩니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napMirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 필요한 SMB 서명을 사용하도록 설정한 경우, 대상 SVM에서 필요한 SMB 서명을 수동으로 활성화해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

SMB 서명이 필요한 경우	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-signing-required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-signing-required false'

2. 다음 명령의 출력에서 "is signing required" 필드의 값이 원하는 값으로 설정되어 있는지 확인하여 필요한 SMB 서명이 활성화되어 있는지 또는 비활성화되어 있는지 확인합니다. 'vserver cifs security show -vserver\_vserver\_name\_-fields is-signing-required'

예

다음 예에서는 SVM VS1 에 필요한 SMB 서명을 활성화합니다.

```
cluster1::> vservers cifs security modify -vservers vs1 -is-signing-required true

cluster1::> vservers cifs security show -vservers vs1 -fields is-signing-required
vservers  is-signing-required
-----  -
vs1       true
```



암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

#### SMB 세션이 서명되었는지 확인합니다

CIFS 서버에서 연결된 SMB 세션에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 SMB 세션이 서명되었는지 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 스토리지 가상 시스템(SVM)에서 서명된 모든 세션	'vservers cifs session show -vservers vservers_name -is-session-signed true'
SVM에서 특정 세션 ID와 서명된 세션의 세부 정보	'vservers cifs session show -vservers vservers_name -session-id integer-instance'

#### 예

다음 명령을 실행하면 SVM VS1 에서 서명된 세션에 대한 세션 정보가 표시됩니다. 기본 요약 출력에는 ""세션 서명됨" 출력 필드가 표시되지 않습니다.

```
cluster1::> vservers cifs session show -vservers vs1 -is-session-signed true
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----  -----  -
3151272279  1          10.1.1.1         DOMAIN\joe        2         23s
```

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 세션의 서명 여부를 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## 관련 정보

### SMB 서명 세션 통계 모니터링

**SMB** 서명 세션 통계를 모니터링합니다

SMB 세션 통계를 모니터링하고 서명된 설정된 세션과 그렇지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 서명된 SMB 세션 수를 모니터링하는 데 사용할 수 있는 'signed\_sessions' 카운터를 제공합니다. 'Signed\_sessions' 카운터는 다음과 같은 통계 객체와 함께 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 세션에 대해 SMB 서명을 모니터링할 수 있습니다.
- 'MB1'을 사용하면 SMB 1.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.
- 'MB2'를 사용하면 SMB 2.x 및 SMB 3.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.

SMB 3.0 통계는 'MB2' 객체의 출력에 포함됩니다.

서명된 세션의 수를 총 세션 수와 비교하려면 'signed\_sessions' 카운터의 출력을 '설정된\_sessions' 카운터의 출력과 비교할 수 있습니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

## 단계

1. 권한 수준을 `advanced:+'et-Privilege advanced`로 설정합니다

2. 데이터 수집 시작:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id  
sample_ID [-node node_name]
```

'-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

3. 'statistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

4. SMB 서명 통계 보기:

에 대한 정보를 보려면...	입력...
서명된 세션	shope-sample-id sample_ID-counter signed_sessions
<i>node_name</i> [-node_node_name_]	서명된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter signed_sessions	ESTANCE_SECURIONS

단일 노드에 대한 정보만 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 2.x 및 SMB 3.0 서명 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 서명된 SMB 세션과 샘플의 노드별 설정된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smb signing_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

다음 명령을 실행하면 샘플에서 노드 2에 대해 서명된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smb signing_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

다음 명령을 실행하면 admin 권한 레벨로 다시 이동됩니다.

```
cluster1::*> set -privilege admin
```

**SMB**를 통한 데이터 전송을 위해 **SMB** 서버에서 필요한 **SMB** 암호화를 구성합니다

#### SMB 암호화 개요

SMB를 통한 데이터 전송을 위한 SMB 암호화는 SMB 서버에서 활성화 또는 비활성화할 수 있는 향상된 보안 기능입니다. 공유 속성 설정을 통해 공유별로 원하는 SMB 암호화 설정을 구성할 수도 있습니다.

기본적으로 SVM(스토리지 가상 머신)에 SMB 서버를 생성할 때 SMB 암호화는 사용하지 않도록 설정됩니다. SMB 암호화를 통해 제공되는 향상된 보안을 활용하려면 이 기능을 활성화해야 합니다.

암호화된 SMB 세션을 생성하려면 SMB 클라이언트가 SMB 암호화를 지원해야 합니다. Windows Server 2012 및 Windows 8부터 시작되는 Windows 클라이언트는 SMB 암호화를 지원합니다.

SVM의 SMB 암호화는 두 가지 설정을 통해 제어됩니다.

- SVM에서 기능을 활성화하는 SMB 서버 보안 옵션
- 공유 단위로 SMB 암호화 설정을 구성하는 SMB 공유 속성입니다

SVM의 모든 데이터에 액세스하려면 암호화를 사용할지, 선택한 공유에서만 데이터에 액세스하려면 SMB 암호화가 필요한지 여부를 결정할 수 있습니다. SVM 레벨 설정이 공유 레벨 설정보다 우선합니다.

효과적인 SMB 암호화 구성은 두 가지 설정의 조합에 따라 달라지며 다음 표에 설명되어 있습니다.

SMB 서버 SMB 암호화가 활성화되었습니다	공유 암호화 데이터 설정이 활성화되었습니다	서버측 암호화 동작
참	거짓	SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
참	참	공유 레벨 암호화와 관계없이 SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
거짓	참	특정 공유에 대해 공유 수준 암호화가 설정됩니다. 이 구성을 사용하면 트리 연결로부터 암호화가 수행됩니다.
거짓	거짓	암호화가 활성화되지 않았습니다.



암호화를 지원하지 않는 SMB 클라이언트는 암호화가 필요한 SMB 서버 또는 공유에 연결할 수 없습니다.

암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

#### **SMB 암호화가 성능에 미치는 영향**

SMB 세션에서 SMB 암호화를 사용하면 Windows 클라이언트와 서버 간의 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버 모두에 영향을 미칩니다(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드).

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 암호화된 SMB 트래픽에서 성능을 향상시킬 수 있습니다. SMB 암호화 오프로드는 SMB 암호화가 활성화된 경우 기본적으로 활성화됩니다.

향상된 SMB 암호화 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 암호화가 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경의 테스트를 통해서만 확인할 수 있습니다.

SMB 서버에서 SMB 암호화는 기본적으로 비활성화되어 있습니다. 암호화가 필요한 SMB 공유 또는 SMB 서버에서만 SMB 암호화를 활성화해야 합니다. SMB 암호화를 통해 ONTAP는 요청을 암호 해독하고 모든 요청에 대한 응답을 암호화하는 추가 처리를 수행합니다. 따라서 필요한 경우에만 SMB 암호화를 활성화해야 합니다.

수신 **SMB** 트래픽에 필요한 **SMB** 암호화를 설정하거나 해제합니다

수신 SMB 트래픽에 SMB 암호화가 필요한 경우 CIFS 서버 또는 공유 레벨에서 설정할 수 있습니다. 기본적으로 SMB 암호화는 필요하지 않습니다.

이 작업에 대해

CIFS 서버에서 SMB 암호화를 설정하면 CIFS 서버의 모든 공유에 적용됩니다. CIFS 서버의 모든 공유에 대해 SMB 암호화가 필요하지 않거나 공유 단위로 수신 SMB 트래픽에 대해 필요한 SMB 암호화를 설정하려는 경우 CIFS 서버에서 필요한 SMB 암호화를 해제할 수 있습니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napmirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 SMB 암호화를 사용하도록 설정한 경우 대상에서 CIFS 서버 SMB 암호화를 수동으로 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

<b>CIFS</b> 서버에서 들어오는 <b>SMB</b> 트래픽에 대해 <b>SMB</b> 암호화가 필요한 경우	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required false'

2. CIFS 서버에서 필요한 SMB 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vserver cifs security show -vserver\_vserver\_name\_-fields is-smb-encryption-required'

CIFS 서버에 필요한 SMB 암호화가 설정되어 있으면 is-smb-encryption-required 필드에 true가 표시되고, 비활성화된 경우에는 false가 표시됩니다.

예

다음 예에서는 SVM VS1에서 CIFS 서버에 대해 수신 SMB 트래픽에 필요한 SMB 암호화를 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----
vs1      true
```

클라이언트가 암호화된 **SMB** 세션을 사용하여 연결되어 있는지 확인합니다

연결된 SMB 세션에 대한 정보를 표시하여 클라이언트가 암호화된 SMB 연결을 사용하는지 여부를 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

SMB 클라이언트 세션은 다음 세 가지 암호화 수준 중 하나를 가질 수 있습니다.

- "암호화되지 않음"

SMB 세션이 암호화되지 않았습니다. SVM(스토리지 가상 시스템) 레벨 또는 공유 레벨 암호화가 구성되지 않았습니다.

- 부분적으로 암호화되었습니다

트리 연결이 발생하면 암호화가 시작됩니다. 공유 수준 암호화가 구성됩니다. SVM 레벨 암호화가 활성화되지 않았습니다.

- '암호화됨'

SMB 세션이 완전히 암호화됩니다. SVM 레벨 암호화가 활성화됩니다. 공유 수준 암호화가 활성화되어 있거나 활성화되어 있지 않을 수 있습니다. SVM 레벨 암호화 설정이 공유 레벨 암호화 설정보다 우선합니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 세션에 대해 지정된 암호화 설정을 갖는 세션	'vserver cifs session show -vserver_vserver_name_{encrypted
sPartially-encrypted	encrypted}-instance'
지정된 SVM에서 특정 세션 ID의 암호화 설정입니다	'vserver cifs session show -vserver_vserver_name_-session-id_integer_-instance'

#### 예

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 암호화 설정을 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

**SMB 암호화 통계를 모니터링합니다**

SMB 암호화 통계를 모니터링하고 설정된 세션 및 공유 연결이 암호화되고 암호화되지 않은

세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 다음 카운터를 제공하며, 이 카운터를 사용하여 암호화된 SMB 세션 수를 모니터링하고 연결을 공유할 수 있습니다.

카운터 이름	설명
'암호화 세션'	암호화된 SMB 3.0 세션의 수를 제공합니다
'암호화_공유_연결'	트리 연결이 발생한 암호화된 공유 수를 제공합니다
"암호화되지 않은 세션"이 끼어들었습니다	에서는 클라이언트 암호화 기능이 부족하여 거부된 세션 설정 수를 제공합니다
"암호화되지 않은_공유"가 있습니다	에서는 클라이언트 암호화 기능이 없어 거부된 공유 매핑 수를 제공합니다

이러한 카운터는 다음 통계 개체에서 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 3.0 세션에 대해 SMB 암호화를 모니터링할 수 있습니다.

SMB 3.0 통계는 'CIFS' 객체의 출력에 포함됩니다. 암호화된 세션의 수를 총 세션 수와 비교하려면 "encrypted\_sessions" 카운터의 출력과 "encrypted\_sessions" 카운터의 출력을 비교할 수 있습니다.

암호화된 공유 연결 수와 총 공유 연결 수를 비교하려면 에 대한 출력을 비교할 수 있습니다 encrypted\_share\_connections 에 대한 출력이 있는 카운터 connected\_shares 카운터.

- reped\_cencrypted\_sessions는 SMB 암호화를 지원하지 않는 클라이언트로부터 암호화를 요구하는 SMB 세션을 설정하려고 시도한 횟수를 제공합니다.
- refened\_cencrypted\_share는 SMB 암호화를 지원하지 않는 클라이언트의 암호화가 필요한 SMB 공유에 연결하려고 시도한 횟수를 제공합니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:'+et-Privilege advanced로 설정합니다

2. 데이터 수집 시작:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

'-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

4. SMB 암호화 통계 보기:

에 대한 정보를 보려면...	입력...
암호화된 세션	'shope-sample-id_sample_ID_-counter encrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter encrypted_sessions	encrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화된 공유 연결
'shope-sample-id_sample_ID_-counter encrypted_share_connections	<i>node_name</i> [-node_node_name_]
암호화된 공유 연결 및 연결된 공유	'sHow-sample-id_sample_ID_-counter encrypted_share_connections
Connected_share	<i>node_name</i> [-node_node_name_]
암호화되지 않은 세션이 거부되었습니다	shope-sample-id_sample_ID_-counter rejected_sencrypted_sessions
<i>node_name</i> [-node_node_name_]	암호화되지 않은 공유 연결이 거부되었습니다
'shd-sample-id_sample_ID_-counter rejected_sencrypted_share	<i>node_name</i> [-node_node_name_]

단일 노드에 대해서만 정보를 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 3.0 암호화 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 해당 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 암호화된 SMB 세션 및 샘플의 노드에 의해 설정된 SMB 세션이 표시됩니다.

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 세션이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

다음 명령을 실행하면 샘플의 노드에 의해 연결된 SMB 공유 및 암호화된 SMB 공유의 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:41:43  
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 공유 연결이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:42:06  
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

관련 정보

[사용할 수 있는 통계 개체 및 카운터 결정](#)

["성능 모니터링 및 관리 개요"](#)

보안 **LDAP** 세션 통신

**LDAP** 서명 및 봉인 개념

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록



서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 CIFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준\_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다.

SVM에서 SVM CIFS 보안 수정 명령에 대한 '-session-security-for-ad-ldap' 옵션을 사용하여 CIFS 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

**CIFS 서버에서 LDAP 서명 및 봉인을 설정합니다**

CIFS 서버가 Active Directory LDAP 서버와의 보안 통신을 위해 서명 및 봉인을 사용하려면 먼저 CIFS 서버 보안 설정을 수정하여 LDAP 서명 및 봉인을 설정해야 합니다.

시작하기 전에

적절한 보안 구성 값을 확인하려면 AD 서버 관리자에게 문의해야 합니다.

단계

1. Active Directory LDAP 서버에서 서명되고 봉인된 트래픽을 사용할 수 있도록 CIFS 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver\_vserver\_name\_-session-security-for-ad-ldap{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.

2. LDAP 서명 및 봉인 보안 설정이 올바르게 설정되었는지 확인합니다. 'vserver cifs security show -vserver\_vserver\_name\_'



SVM이 이름 매핑 또는 사용자, 그룹, 넷그룹과 같은 기타 UNIX 정보를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령의 '-session-security' 옵션을 사용하여 해당 설정을 활성화해야 합니다.

**TLS를 통해 LDAP를 구성합니다**

자체 서명된 루트 **CA** 인증서의 복사본을 내보냅니다

Active Directory 통신을 보호하기 위해 SSL/TLS를 통한 LDAP를 사용하려면 먼저 Active Directory 인증서 서비스의 자체 서명 루트 CA 인증서 복사본을 인증서 파일로 내보내고 ASCII 텍스트 파일로 변환해야 합니다. 이 텍스트 파일은 ONTAP에서 SVM(스토리지 가상 머신)에 인증서를 설치하는 데 사용됩니다.

시작하기 전에

CIFS 서버가 속한 도메인에 대해 Active Directory 인증서 서비스가 이미 설치 및 구성되어 있어야 합니다. Active Director 인증서 서비스 설치 및 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

"Microsoft TechNet 라이브러리: [technet.microsoft.com](http://technet.microsoft.com)"

단계

1. '.pem' 텍스트 형식인 도메인 컨트롤러의 루트 CA 인증서를 얻습니다.

작업을 마친 후

SVM에 인증서를 설치합니다.

관련 정보

"Microsoft TechNet 라이브러리"

**SVM**에 자체 서명된 루트 **CA** 인증서를 설치합니다

LDAP 서버에 바인딩할 때 TLS를 사용한 LDAP 인증이 필요한 경우 먼저 SVM에 자체 서명된 루트 CA 인증서를 설치해야 합니다.

이 작업에 대해

TLS를 통한 LDAP가 활성화된 경우 SVM의 ONTAP LDAP 클라이언트는 ONTAP 9.0 및 9.1에서 해지된 인증서를 지원하지 않습니다.

ONTAP 9.2부터 TLS 통신을 사용하는 ONTAP 내의 모든 응용 프로그램은 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 디지털 인증서 상태를 확인할 수 있습니다. OCSP가 TLS를 통해 LDAP에 대해 활성화된 경우 해지된 인증서가 거부되고 연결이 실패합니다.

단계

1. 자체 서명된 루트 CA 인증서 설치:

a. 인증서 설치를 시작합니다. 'Security certificate install - vserver vserver\_name -type server -ca'

콘솔 출력에는 'Please enter Certificate: press <Enter> when done(인증서를 입력하십시오. 완료되면 <Enter> 키를 누르십시오)' 메시지가 표시됩니다

b. 텍스트 편집기로 인증서 '.pem' 파일을 열고 '-----'로 시작하는 줄을 포함하여 인증서를 복사합니다. 인증서 시작 -----'로 끝나는 종료 인증서 ----- 그런 다음 명령 프롬프트 뒤에 인증서를 붙여 넣습니다.

c. 인증서가 올바르게 표시되는지 확인합니다.

d. Enter 키를 눌러 설치를 완료합니다.

2. 인증서가 설치되어 있는지 확인합니다. 'Security certificate show -vserver\_vserver\_name\_'

서버에서 **TLS**를 통해 **LDAP**를 활성화합니다

SMB 서버가 Active Directory LDAP 서버와의 보안 통신에 TLS를 사용하려면 먼저 SMB 서버 보안 설정을 수정하여 TLS를 통한 LDAP를 활성화해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 AD(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. AD 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 설정하려면 'vserver cifs security modify ' 명령을 사용하여 '-try-channel-binding-for-ad-ldap' 매개 변수를 사용합니다.

자세한 내용은 다음을 참조하십시오.

- "[LDAP 개요](#)"

- "Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

## 단계

1. Active Directory LDAP 서버와 보안 LDAP 통신을 허용하는 SMB 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver\_vserver\_name\_-use-start-tls-for-ad-ldap true'
2. TLS를 통한 LDAP 보안 설정이 "true"로 설정되어 있는지 확인합니다. vserver cifs security show -vserver\_vserver\_name\_



SVM이 이름 매핑 또는 기타 UNIX 정보(예: 사용자, 그룹 및 넷그룹)를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령을 사용하여 '-use-start-tls' 옵션도 수정해야 합니다.

## 성능 및 이중화를 위해 **SMB** 멀티 채널을 구성합니다

ONTAP 9.4부터 SMB 다중 채널을 구성하여 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 연결을 제공할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다.

### 시작하기 전에

SMB 3.0 이상 버전에서 클라이언트가 협상하는 경우에만 SMB 멀티 채널 기능을 사용할 수 있습니다. SMB 3.0 이상은 기본적으로 ONTAP SMB 서버에서 사용하도록 설정됩니다.

### 이 작업에 대해

ONTAP 클러스터에서 적절한 구성이 식별되는 경우 SMB 클라이언트가 자동으로 여러 네트워크 연결을 감지하고 사용합니다.

SMB 세션의 동시 연결 수는 구축한 NIC에 따라 달라집니다.

- \* 클라이언트와 ONTAP 클러스터의 1G NIC \*

클라이언트는 NIC당 하나의 연결을 설정하고 모든 연결에 세션을 바인딩합니다.

- \* 클라이언트 및 ONTAP 클러스터에 10G 이상의 대용량 NIC \*

클라이언트는 NIC당 최대 4개의 연결을 설정하고 모든 연결에 세션을 바인딩합니다. 클라이언트는 여러 개의 10G 및 대용량 NIC에 연결을 설정할 수 있습니다.

다음 매개 변수(고급 권한)도 수정할 수 있습니다.

- \* '-max-connections-per-session' \*

다중 채널 세션당 허용되는 최대 연결 수입니다. 기본값은 32개 연결입니다.

기본값보다 더 많은 연결을 설정하려면 기본값인 32개의 연결을 사용하는 클라이언트 구성을 동일하게 조정해야 합니다.

- \* '-max-liff-per-session' \*

Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 기본값은 256개의 네트워크 인터페이스입니다.

## 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. SMB 서버에서 SMB 멀티 채널 활성화: 'vserver cifs options modify -vserver\_vserver\_name\_-is-multichannel -enabled true
3. ONTAP가 SMB 멀티 채널 세션을 보고하는지 확인합니다. 'vserver cifs session show\_options\_'
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

## 예

다음 예에서는 모든 SMB 세션에 대한 정보를 표시하며 단일 세션에 대해 여러 개의 연결을 표시합니다.

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                                Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1      DOMAIN\
4s
Administrator
```

다음 예에서는 세션 ID 1이 있는 SMB 세션에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

## SMB 서버에서 기본 **Windows** 사용자를 **UNIX** 사용자 매핑으로 구성합니다

### 기본 **UNIX** 사용자를 구성합니다

기본 UNIX 사용자는 사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우에 사용하도록 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 UNIX 사용자를 구성하지 않아야 합니다.

#### 이 작업에 대해

기본적으로 기본 UNIX 사용자의 이름은 "pcuser"입니다. 즉, 기본적으로 기본 UNIX 사용자에 대한 사용자 매핑이 설정됩니다. 기본 UNIX 사용자로 사용할 다른 이름을 지정할 수 있습니다. 지정하는 이름은 SVM(스토리지 가상 머신)용으로 구성된 네임 서비스 데이터베이스에 있어야 합니다. 이 옵션이 null 문자열로 설정된 경우 CIFS 서버를 UNIX 기본 사용자로 액세스할 수 없습니다. 즉, 각 사용자는 CIFS 서버를 액세스하기 전에 암호 데이터베이스에 계정이 있어야 합니다.

사용자가 기본 UNIX 사용자 계정을 사용하여 CIFS 서버에 접속하려면 다음과 같은 사전 요구 사항을 충족해야 합니다.

- 사용자가 인증됩니다.
- 사용자가 CIFS 서버의 로컬 Windows 사용자 데이터베이스, CIFS 서버의 홈 도메인 또는 신뢰할 수 있는 도메인에 있습니다(CIFS 서버에서 다중 도메인 이름 매핑 검색이 설정된 경우).
- 사용자 이름이 null 문자열에 명시적으로 매핑되어 있지 않습니다.

#### 단계

## 1. 기본 UNIX 사용자 구성:

원하는 작업	입력...
기본 UNIX 사용자 ""pcuser"" 사용	'vserver cifs options modify-default-unix-user pcuser'
다른 UNIX 사용자 계정을 기본 사용자로 사용합니다	'vserver cifs options modify-default-unix-user _user_name_ '
기본 UNIX 사용자를 비활성화합니다	'vserver cifs options modify-default-unix-user''

'vserver cifs options modify-default-unix-user pcuser'

## 2. 기본 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver \_vserver\_name\_ '

다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

## 게스트 UNIX 사용자를 구성합니다

게스트 UNIX 사용자 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 게스트 UNIX 사용자에게 매핑되고 CIFS 서버에 연결할 수 있습니다. 또는 신뢰할 수 없는 도메인의 사용자 인증에 실패하도록 하려면 게스트 UNIX 사용자를 구성하지 않아야 합니다. 기본값은 신뢰할 수 없는 도메인의 사용자가 CIFS 서버에 접속할 수 없도록 하는 것입니다(게스트 UNIX 계정이 구성되지 않음).

이 작업에 대해

게스트 UNIX 계정을 구성할 때 다음 사항을 염두에 두어야 합니다.

- CIFS 서버가 홈 도메인 또는 신뢰할 수 있는 도메인 또는 로컬 데이터베이스에 대한 도메인 컨트롤러에 대해 사용자를 인증할 수 없고 이 옵션이 설정된 경우 CIFS 서버는 사용자를 게스트 사용자로 간주하고 지정된 UNIX 사용자에게 매핑합니다.
- 이 옵션을 null 문자열로 설정하면 게스트 UNIX 사용자가 비활성화됩니다.

- SVM(Storage Virtual Machine) 이름 서비스 데이터베이스 중 하나에서 게스트 UNIX 사용자로 사용할 UNIX 사용자를 생성해야 합니다.
- 게스트 사용자로 로그인한 사용자는 자동으로 CIFS 서버에 있는 BUILTIN\guests 그룹의 구성원입니다.
- 'homedirs-public' 옵션은 인증된 사용자에게만 적용됩니다. 게스트 사용자로 로그인한 사용자는 홈 디렉토리가 없으며 다른 사용자의 홈 디렉토리에 액세스할 수 없습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	입력...
게스트 UNIX 사용자를 구성합니다	'vserver cifs options modify-guest-unix-user _unix_name_'
게스트 UNIX 사용자를 비활성화합니다	'vserver cifs options modify-guest-unix-user''

'vserver cifs options modify-guest-unix-user pcuser'

2. 게스트 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver \_vserver\_name\_'

다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

관리자 그룹을 루트에 매핑합니다

사용자 환경에 CIFS 클라이언트만 있고 SVM(스토리지 가상 시스템)을 멀티프로토콜 스토리지 시스템으로 설정한 경우, SVM에서 파일에 액세스할 수 있는 루트 권한이 있는 Windows 계정이 하나 이상 있어야 합니다. 그렇지 않으면 충분한 사용자 권한이 없기 때문에 SVM을 관리할 수 없습니다.

이 작업에 대해

그러나 스토리지 시스템이 NTFS 전용으로 설정된 경우, '/etc' 디렉토리에는 관리자 그룹이 ONTAP 구성 파일에 액세스할 수 있도록 하는 파일 레벨 ACL이 있습니다.

## 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 관리자 그룹을 루트에 적절하게 매핑하는 CIFS 서버 옵션을 구성합니다.

원하는 작업	그러면...
관리자 그룹 구성원을 루트에 매핑합니다	'vserver cifs options modify -vserver_vserver_name_-is-admin-users-mapped-to-root-enabled true' 계정을 루트로 매핑하는 '/etc/usermap.cfg' 항목이 없는 경우에도 administrators 그룹의 모든 계정은 루트로 간주됩니다. administrators 그룹에 속하는 계정을 사용하여 파일을 생성하는 경우 UNIX 클라이언트에서 파일을 볼 때 파일은 루트에서 소유합니다.
관리자 그룹 구성원을 루트에 매핑하도록 해제합니다	"vserver cifs options modify -vserver_vserver_name_-is-admin-users-mapped-to-root-enabled false" administrators 그룹의 계정은 더 이상 루트에 매핑되지 않습니다. 단일 사용자만 루트에 명시적으로 매핑할 수 있습니다.

3. 옵션이 원하는 값('vserver cifs options show -vserver\_vserver\_name\_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

## SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시합니다

SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시할 수 있습니다. 따라서 적절한 유형의 사용자만 SVM(스토리지 가상 머신)의 SMB 세션을 통해 연결할 수 있습니다.

이 작업에 대해

다음 유형의 사용자는 SMB 세션을 통해 연결할 수 있습니다.

- '로컬 사용자'

로컬 CIFS 사용자로 인증되었습니다

- '다민 사용자'입니다

도메인 사용자로 인증됨(CIFS 서버의 홈 도메인 또는 신뢰할 수 있는 도메인)

- 'guest-user'입니다

게스트 사용자로 인증되었습니다

- 익명의 사용자

익명 또는 null 사용자로 인증되었습니다

## 단계



1. SMB 세션을 통해 연결된 사용자 유형을 확인합니다. 'vserver cifs session show -vserver\_vserver\_name\_-windows-user\_windows\_user\_name\_-fields windows-user, address, lif-address, user-type'

설정된 세션에 대한 사용자 유형 정보를 표시하려면...	다음 명령을 입력합니다...
사용자 유형이 지정된 모든 세션에 대해	'vserver cifs session show -vserver_vserver_name_-user-type{local-user
domain-user	guest-user
anonymous-user}'입니다	특정 사용자의 경우

예

다음 명령을 실행하면 ""iepubs\user1" 사용자가 설정한 SVM VS1 세션의 사용자 유형에 대한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node          vserver session-id connection-id lif-address  address
windows-user          user-type
-----
pub1node1 pub1      1          3439441860      10.0.0.1      10.1.1.1
IEPUBS\user1          domain-user
```

과도한 **Windows** 클라이언트 리소스 사용을 제한하는 명령 옵션입니다

'vserver cifs options modify' 명령 옵션을 사용하면 Windows 클라이언트의 리소스 사용을 제어할 수 있습니다. 이 기능은 클라이언트가 리소스 사용의 정상적인 범위를 벗어난 경우(예: 열려 있는 파일의 수가 비정상적으로 많거나 세션이 열려 있거나 변경 알림 요청이 있는 경우) 유용합니다.

Windows 클라이언트 리소스 사용을 제어하기 위해 'vserver cifs options modify' 명령에 대한 다음 옵션이 추가되었습니다. 이 옵션 중 최대값이 초과되면 요청이 거부되고 EMS 메시지가 전송됩니다. 이 옵션에 대해 구성된 제한값의 80%에 도달하면 EMS 경고 메시지도 전송됩니다.

- '-max-오픈-파일-트리 단위'

CIFS 트리당 동일한 파일에 대한 최대 열기 수입니다

- '-max-same-user-sessions-per-connection'

동일한 사용자가 접속당 연 최대 세션 수입니다

- '-max-same-tree-connect-per-session'

세션당 동일한 공유에 대한 최대 트리 연결 수입니다

- '-max-s워치-세트당-트리'

트리당 설정된 최대 시계 수(\_CHANGE ALBERS\_라고도 함)입니다

기본 제한 및 현재 구성을 표시하려면 man 페이지를 참조하십시오.

ONTAP 9.4부터 SMB 버전 2 이상을 실행하는 서버는 클라이언트가 SMB 연결을 통해 서버로 전송할 수 있는 미해결 요청(*smb* 크레딧) 수를 제한할 수 있습니다. SMB 크레딧의 관리는 클라이언트가 시작하고 서버에 의해 제어됩니다.

SMB 연결에서 허용할 수 있는 최대 요청 수는 '-max-credits' 옵션으로 제어됩니다. 이 옵션의 기본값은 128입니다.

## 기존 **oplocks** 및 리스 **oplocks**로 클라이언트 성능 향상

기존 및 리스 **oplocks** 개요를 통해 클라이언트 성능 향상

기존 oplocks(기회 잠금) 및 리스 oplocks는 특정 파일 공유 시나리오에서 SMB 클라이언트가 미리 읽기, 쓰기 후 및 잠금 정보의 클라이언트측 캐싱을 수행할 수 있도록 합니다. 그러면 클라이언트는 해당 파일에 액세스해야 한다는 사실을 서버에 정기적으로 알려주지 않고 파일을 읽거나 파일에 쓸 수 있습니다. 이렇게 하면 네트워크 트래픽이 줄어들어 성능이 향상됩니다.

리스 oplocks는 SMB 2.1 프로토콜 이상에서 사용할 수 있는 향상된 형태의 oplocks입니다. 리스 oplocks를 사용하면 클라이언트가 자체적으로 시작된 여러 SMB에서 클라이언트 캐싱 상태를 확보하고 유지할 수 있습니다.

oplocks는 다음 두 가지 방법으로 제어할 수 있습니다.

- 공유를 생성할 때 공유 속성에 의해 'vserver cifs share create' 명령을 사용하거나 생성 후 'vserver share properties' 명령을 사용합니다.
- qtree가 생성될 때 'volume qtree create' 명령을 사용하거나 생성 후 'volume qtree oplock' 명령을 사용하여 qtree 속성에 의해 생성됩니다.

## **oplocks** 사용 시 캐시 데이터 손실 고려 사항 쓰기

경우에 따라 프로세스에 파일에 배타적 oplock이 있고 두 번째 프로세스에서 파일을 열려고 시도할 경우 첫 번째 프로세스에서는 캐시된 데이터를 무효화하고 쓰기 및 잠금을 플러시해야 합니다. 그런 다음 클라이언트는 oplock 및 파일에 대한 액세스를 양도해야 합니다. 이 플러시 중에 네트워크 장애가 발생하면 캐시된 쓰기 데이터가 손실될 수 있습니다.

- 데이터 손실 가능성

다음과 같은 상황에서는 쓰기 캐싱된 데이터가 있는 모든 애플리케이션에서 해당 데이터가 손실될 수 있습니다.

- 연결은 SMB 1.0을 사용하여 이루어집니다.
- 파일에 배타적 oplock이 있습니다.
- 해당 oplock을 깨거나 파일을 닫도록 합니다.
- 쓰기 캐시를 플러시하는 프로세스 중에 네트워크 또는 타겟 시스템에서 오류가 발생합니다.

- 오류 처리 및 쓰기 완료

캐시 자체는 오류 처리를 하지 않습니다. 애플리케이션에서 캐시에 쓰기를 수행할 때는 항상 쓰기가 완료됩니다. 캐시가 네트워크를 통해 타겟 시스템에 쓰기를 수행하는 경우 쓰기가 완료된 것으로 가정해야 합니다. 그렇지 않으면 데이터가 손실되기 때문입니다.

## SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다

oplocks를 사용하면 클라이언트가 파일을 잠그고 콘텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. oplocks는 스토리지 가상 시스템(SVM)에 상주하는 SMB 공유에 설정됩니다. 경우에 따라 oplocks를 해제할 수 있습니다. 공유별로 oplocks를 설정하거나 해제할 수 있습니다.



### 이 작업에 대해

공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 해제됩니다. 공유에서 oplocks를 비활성화하면 볼륨 oplock 설정보다 우선적으로 적용됩니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다.

심표로 구분된 목록을 사용하여 oplock 공유 속성을 지정하는 것 외에도 다른 공유 속성을 지정할 수 있습니다. 다른 공유 매개 변수를 지정할 수도 있습니다.

### 단계

- 해당 작업을 수행합니다.

원하는 작업	그러면...
공유를 생성하는 동안 공유에 oplocks를 설정합니다	<div>'vserver cifs share create -vserver_vserver_name_-share-name share_name -path path_to_share-share-properties [oplocks,...]' 명령을 입력합니다</div> <div> <div></div> <div>공유에서 oplocks, browsable, changentify의 기본 공유 속성만 사용하려면 SMB 공유를 생성할 때 '-share-properties' 매개 변수를 지정하지 않아도 됩니다. 기본값 이외의 공유 속성을 조합하려면 해당 공유에 사용할 공유 속성 목록과 함께 '-share-properties' 매개 변수를 지정해야 합니다.</div> </div>
공유를 생성하는 동안 공유에 oplocks를 사용하지 않도록 설정합니다	<div>'vserver cifs share create-vserver_vserver_name_-share-name_share_name_-path_to_share_-share-properties[other_share_property,...]' 명령을 입력합니다</div> <div> <div></div> <div>oplocks를 해제할 때는 공유를 생성할 때 공유 속성 목록을 지정해야 하지만 "oplocks" 속성을 지정해서는 안 됩니다.</div> </div>

### 관련 정보

## 기존 SMB 공유에서 oplocks 설정 또는 해제

### oplock 상태 모니터링

볼륨 및 **qtree**에서 **oplocks**를 설정하거나 해제하는 명령입니다

oplocks를 사용하면 클라이언트가 파일을 잠그고 콘텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. 볼륨 또는 qtree에서 oplocks를 설정하거나 해제하는 명령을 알아야 합니다. 또한 볼륨 및 qtree에서 oplocks를 설정하거나 해제할 수 있는 시기를 알아야 합니다.

- oplocks는 기본적으로 볼륨에 설정됩니다.
- 볼륨을 생성할 때는 oplocks를 해제할 수 없습니다.
- 언제든지 기존 볼륨에서 SVM에 대한 oplocks를 설정하거나 해제할 수 있습니다.
- SVM에 대해 qtree에서 oplocks를 설정할 수 있습니다.

oplock 모드 설정은 qtree ID 0의 속성으로, 모든 볼륨에 있는 기본 qtree입니다. qtree를 생성할 때 oplock 설정을 지정하지 않으면 qtree가 기본적으로 사용되는 상위 볼륨의 oplock 설정을 상속합니다. 그러나 새 qtree에 oplock 설정을 지정하면 볼륨의 oplock 설정보다 우선합니다.

원하는 작업	이 명령 사용...
볼륨 또는 qtree에 oplocks를 설정합니다	'-oplock-mode' 매개 변수가 'enable'로 설정된 볼륨 qtree oplocks
볼륨 또는 qtree에서 oplocks를 해제합니다	'-oplock-mode' 매개 변수가 '사용할 수 있음'으로 설정된 볼륨 qtree oplocks입니다

### 관련 정보

### oplock 상태 모니터링

기존 **SMB** 공유에서 **oplocks**를 설정하거나 해제합니다



oplocks는 기본적으로 스토리지 가상 시스템(SVM)의 SMB 공유에 설정됩니다. 경우에 따라 oplocks를 해제할 수도 있습니다. 이전에 공유에서 oplocks를 해제한 경우에는 oplocks를 다시 설정할 수도 있습니다.

### 이 작업에 대해

공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 비활성화됩니다. 공유에 oplocks를 사용하지 않도록 설정하면 볼륨에서 oplocks를 설정하는 것이 우선합니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다. 언제든지 기존 공유에 oplocks를 설정하거나 해제할 수 있습니다.

### 단계

1. 해당 작업을 수행합니다.

원하는 작업	그러면...
기존 공유를 수정하여 공유에 oplocks를 설정합니다	<p>'vserver cifs share properties add -vserver_vserver_name_-share-name share_name-share-properties oplocks' 명령을 입력합니다</p> <div>  <p>쉼표로 구분된 목록을 사용하여 추가할 추가 공유 속성을 지정할 수 있습니다.</p> </div> <p>새로 추가된 속성은 기존 공유 속성 목록에 추가됩니다. 이전에 지정한 공유 속성은 그대로 유지됩니다.</p>
기존 공유를 수정하여 공유에 oplocks를 사용하지 않도록 설정합니다	<p>'vserver cifs share properties remove-vserver_vserver_name_-share-name share_name_-share-properties oplocks' 명령을 입력합니다</p> <div>  <p>쉼표로 구분된 목록을 사용하여 제거할 추가 공유 속성을 지정할 수 있습니다.</p> </div> <p>제거한 공유 속성은 기존 공유 속성 목록에서 삭제되지만 이전에 구성한 공유 속성은 제거하지 않습니다.</p>

## 예

다음 명령을 실행하면 스토리지 가상 시스템(SVM, 이전 명칭 Vserver) VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 설정됩니다.

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver      Share      Properties
-----
vs1          Engineering oplocks
              browsable
              changenotify
              showsnapshot
```

다음 명령을 실행하면 SVM VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 해제됩니다.

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	browsable changenotify showsnapshot

## 관련 정보

[SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다](#)

[oplock 상태 모니터링](#)

[기존 SMB 공유에서 공유 속성 추가 또는 제거](#)

## oplock 상태를 모니터링합니다

oplock 상태에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보를 사용하여 oplocks가 있는 파일, oplock 레벨 및 oplock 상태 수준이 무엇인지, oplock 리스가 사용되는지 여부를 확인할 수 있습니다. 수동으로 해제해야 하는 잠금에 대한 정보를 확인할 수도 있습니다.

### 이 작업에 대해

모든 oplocks에 대한 정보를 요약 양식 또는 세부 목록 양식에 표시할 수 있습니다. 선택적 매개 변수를 사용하여 기존 잠금의 하위 집합에 대한 정보를 표시할 수도 있습니다. 예를 들어, 지정된 클라이언트 IP 주소 또는 지정된 경로를 사용하여 출력 반환만 잠그도록 지정할 수 있습니다.

기존 및 리스 oplocks에 대한 다음 정보를 표시할 수 있습니다.

- oplock이 설정된 SVM, 노드, 볼륨 및 LIF입니다
- UUID를 잠급니다
- oplock을 사용하는 클라이언트의 IP 주소입니다
- oplock이 설정된 경로입니다
- 잠금 프로토콜(SMB) 및 유형(oplock)
- 잠금 상태
- oplock 레벨
- 연결 상태 및 SMB 만료 시간입니다
- 임대 oplock이 부여된 경우 그룹 ID를 엽니다

각 매개변수에 대한 자세한 설명은 'vservers oplocks show' man 페이지를 참조하십시오.

### 단계

1. 'vservers lock show' 명령을 사용하여 oplock 상태를 표시합니다.

예

다음 명령을 실행하면 모든 잠금에 대한 기본 정보가 표시됩니다. 표시된 파일의 oplock은 "임시 배치" oplock 레벨로 허가됩니다.

```
cluster1::> vsriver locks show
```

Vserver: vs0

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1			
			cifs	share-level	192.168.1.5
	Sharelock Mode: read_write-deny_delete				
				op-lock	192.168.1.5
	Oplock Level: read-batch				

다음 예제는 경로 '/data2/data2\_2/intro.pptx'를 사용하여 파일의 잠금에 대한 자세한 정보를 표시합니다. IP 주소가 10.3.1.3 인 클라이언트에 배치 oplock 레벨이 있는 파일에 리스 oplock이 부여됩니다.



자세한 정보를 표시할 때 이 명령은 oplock 및 sharelock 정보에 대한 별도의 출력을 제공합니다. 이 예제는 oplock 섹션의 출력만 보여 줍니다.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
    Volume: data2_2
  Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
    Lock Protocol: cifs
    Lock Type: op-lock
  Node Holding Lock State: node3
    Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
  Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
  SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## 관련 정보

[SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다](#)

[기존 SMB 공유에서 oplocks 설정 또는 해제](#)

[볼륨 및 qtree에서 oplocks를 설정하거나 해제하는 명령입니다](#)

## SMB 서버에 그룹 정책 개체를 적용합니다

### SMB 서버에 그룹 정책 개체 적용 개요

SMB 서버는 Active Directory 환경의 컴퓨터에 적용되는 \_group 정책 특성\_이라는 규칙 집합인 GPO(그룹 정책 개체)를 지원합니다. GPO를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM(스토리지 가상 머신)에 대한 설정을 중앙에서 관리할 수 있습니다.

SMB 서버에서 GPO를 사용하도록 설정하면 ONTAP가 GPO 정보를 요청하는 Active Directory 서버에 LDAP 쿼리를 보냅니다. SMB 서버에 적용할 수 있는 GPO 정의가 있는 경우 Active Directory 서버는 다음 GPO 정보를 반환합니다.



- GPO 이름입니다
- 현재 GPO 버전입니다
- GPO 정의의 위치입니다
- GPO 정책 집합에 대한 UUID(Universally Unique Identifier) 목록입니다

#### 관련 정보

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)

#### "SMB 및 NFS 감사 및 보안 추적"

#### 지원되는 GPO

모든 GPO(그룹 정책 개체)가 CIFS 지원 SVM(스토리지 가상 머신)에 적용되는 것은 아니지만 SVM은 관련 GPO 세트를 인식하고 처리할 수 있습니다.

현재 SVM에서 지원되는 GPO는 다음과 같습니다.

- 고급 감사 정책 구성 설정:

객체 액세스: 중앙 액세스 정책 스테이징

다음 설정을 포함하여 중앙 액세스 정책(CAP) 스테이징에 대해 감사할 이벤트 유형을 지정합니다.

- 감사 금지
- 성공 이벤트만 감사합니다
- 오류 이벤트만 감사합니다
- 성공 및 실패 이벤트를 모두 감사합니다



세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

Advanced Audit Policy Configuration/Audit Policies/Object Access GPO에서 Audit Central Access Policy Staging 설정을 이용하여 설정한다.



고급 감사 정책 구성 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 대해 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 레지스트리 설정:

- CIFS 지원 SVM에 대한 그룹 정책 업데이트 간격

레지스트리 GPO를 사용하여 설정합니다.

- 그룹 정책 무작위 오프셋을 새로 고칩니다

레지스트리 GPO를 사용하여 설정합니다.

◦ BranchCache에 대한 해시 게시

BranchCache GPO의 해시 게시는 BranchCache 운영 모드에 해당합니다. 지원되는 세 가지 작동 모드가 지원됩니다.

- 공유당
- 전체 공유
- '레지스트리' GPO를 사용하여 설정을 비활성화했습니다.

◦ BranchCache에 대한 해시 버전 지원

다음 세 가지 해시 버전 설정이 지원됩니다.

- BranchCache 버전 1
- BranchCache 버전 2
- BranchCache 버전 1 및 2는 레지스트리 GPO를 사용하여 설정합니다.



BranchCache GPO 설정을 사용하려면 이러한 설정을 적용할 CIFS 지원 SVM에 BranchCache를 구성해야 합니다. SVM에 BranchCache가 구성되어 있지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

• 보안 설정

◦ 감사 정책 및 이벤트 로그

- 로그인 이벤트를 감사합니다

다음 설정을 포함하여 감사할 로그인 이벤트의 유형을 지정합니다.

- 감사 금지
- 성공 이벤트만 감사합니다
- 장애 이벤트 감사
- Local Policies/Audit Policy GPO에서 Audit logon events 설정을 이용하여 성공 및 실패 이벤트를 모두 Audit한다.



세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

- 개체 액세스를 감사합니다

다음 설정을 포함하여 감사할 개체 액세스 유형을 지정합니다.

- 감사 금지
- 성공 이벤트만 감사합니다
- 장애 이벤트 감사
- Local Policies/Audit Policy GPO의 Audit object access 설정을 이용하여 성공 이벤트와 실패 이벤트를 모두 Audit한다.



세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

- 로그 보존 방법입니다

다음 설정을 포함하여 감사 로그 보존 방법을 지정합니다.

- 로그 파일의 크기가 최대 로그 크기를 초과할 경우 이벤트 로그를 덮어씁니다
- 이벤트 로그 GPO의 보안 로그 보관 방법 설정을 사용하여 이벤트 로그(수동으로 로그 지우기) 집합을 덮어쓰지 마십시오.

- 최대 로그 크기입니다

감사 로그의 최대 크기를 지정합니다.

이벤트 로그 GPO에서 최대 보안 로그 크기 설정을 사용하여 설정합니다.



감사 정책 및 이벤트 로그 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 파일 시스템 보안

GPO를 통해 파일 보안을 적용할 파일 또는 디렉터리 목록을 지정합니다.

파일 시스템 GPO를 사용하여 설정합니다.



파일 시스템 보안 GPO를 구성하는 볼륨 경로가 SVM 내에 있어야 합니다.

- Kerberos 정책

- 최대 클럭 불균형

컴퓨터 시계 동기화에 대한 최대 허용 시간(분)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 컴퓨터 시계 동기화에 대한 최대 허용 한도를 사용하여 설정합니다.

- 최대 항공권 사용 기간

사용자 티켓의 최대 수명(시간)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 사용자 티켓의 최대 수명 설정을 사용하여 설정합니다.

- 최대 티켓 갱신 기간

사용자 티켓 갱신에 대한 최대 수명(일)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 사용자 티켓 갱신을 위한 최대 수명 설정을 사용하여 설정합니다.

- 사용자 권한 할당(권한 권한)

- 소유권 가져오기

보안 개체의 소유권을 가져올 권한이 있는 사용자 및 그룹 목록을 지정합니다.

Local Policies/User Rights Assignment GPO에서 파일 또는 기타 개체의 소유권 가져오기 설정을 사용하여 설정합니다.

- 보안 권한

파일, 폴더 및 Active Directory 개체와 같은 개별 리소스의 개체 액세스에 대한 감사 옵션을 지정할 수 있는 사용자 및 그룹 목록을 지정합니다.

Local Policies/User Rights Assignment GPO에서 MManage auditing and security log 설정을 이용하여 설정한다.

- 알림 권한 변경(통과 확인 무시)

사용자 및 그룹에 통과 디렉터리에 대한 권한이 없더라도 디렉터리 트리를 통과할 수 있는 사용자 및 그룹 목록을 지정합니다.

사용자가 파일 및 디렉토리의 변경 알림을 수신하는 경우에도 동일한 권한이 필요합니다. Local Policies/User Rights Assignment GPO에서 통과 확인 무시 설정을 사용하여 설정합니다.

- 레지스트리 값

- 서명 필요 설정

필요한 SMB 서명을 설정 또는 해제할지 여부를 지정합니다.

보안 옵션 GPO의 'Microsoft 네트워크 서버: 디지털 서명 통신(항상)' 설정을 사용하여 설정합니다.

- 익명 제한

익명 사용자의 제한 사항을 지정하고 다음 세 가지 GPO 설정을 포함합니다.

- SAM(보안 계정 관리자) 계정의 열거 없음:

이 보안 설정은 컴퓨터에 대한 익명 연결에 대해 부여되는 추가 권한을 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 설정을 사용하여 설정합니다.

- SAM 계정 및 공유의 열거 없음

이 보안 설정은 SAM 계정과 공유의 익명 열거가 허용되는지 여부를 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts and 공유 설정을 이용하여 설정한다.

- 공유 및 명명된 파이프에 대한 익명 액세스를 제한합니다

이 보안 설정은 공유 및 파이프에 대한 익명 액세스를 제한합니다. 이 옵션이 활성화된 경우 ONTAP에서 이 옵션이 "no-access"로 표시됩니다.

Local Policies/Security Options GPO에서 Network access: restrict anonymous access to named pipes and Shares 설정을 이용하여 설정한다.

정의된 그룹 정책과 적용된 그룹 정책에 대한 정보를 표시할 때 "익명 사용자에게 대한 결과 제한" 출력 필드는 세 가지 익명 GPO 제한 설정의 결과 제한에 대한 정보를 제공합니다. 가능한 결과 제한은 다음과 같습니다.

- "접근 불가"

익명 사용자는 지정된 공유 및 명명된 파이프에 대한 액세스가 거부되며 SAM 계정과 공유의 열거를 사용할 수 없습니다. 네트워크 액세스: 명명된 파이프 및 공유에 대한 익명 액세스 제한 GPO가 설정된 경우 이러한 제한이 나타납니다.

- 번호 매기기

익명 사용자는 지정된 공유 및 명명된 파이프에 액세스할 수 있지만 SAM 계정과 공유의 열거를 사용할 수는 없습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

- 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
- Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 또는 Network access: do not allow anonymous enumeration of SAM accounts and 공유 GPO(SAM 계정과 공유의 익명 열거 허용 안 함) 중 하나가 활성화됩니다.

- 무제한입니다

익명 사용자는 모든 액세스 권한이 있으며 열거형을 사용할 수 있습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

- 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
- Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 및 Network access: do not allow anonymous enumeration of SAM accounts and ses(SAM 계정과 공유의 익명 열거 허용 안 함) GPO가 모두 비활성화됩니다.
- 제한된 그룹

제한된 그룹을 구성하여 기본 제공 그룹 또는 사용자 정의 그룹의 구성원을 중앙에서 관리할 수 있습니다. 그룹 정책을 통해 제한된 그룹을 적용하면 CIFS 서버 로컬 그룹의 구성원은 적용된 그룹 정책에 정의된 멤버 자격 목록 설정과 일치하도록 자동으로 설정됩니다.

제한 그룹 GPO를 사용하여 설정합니다.

- 중앙 액세스 정책 설정

중앙 액세스 정책 목록을 지정합니다. 중앙 액세스 정책과 관련 중앙 액세스 정책 규칙에 따라 SVM의 여러 파일에 대한 액세스 권한이 결정됩니다.

## 관련 정보

[CIFS 서버에서 GPO 지원을 설정하거나 해제합니다](#)

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)

["SMB 및 NFS 감사 및 보안 추적"](#)

CIFS 서버 Kerberos 보안 설정을 수정합니다

BranchCache를 사용하여 지사에 SMB 공유 콘텐츠를 캐싱합니다

SMB 서명을 사용하여 네트워크 보안을 강화합니다

통과 확인 우회 구성

익명 사용자에게 대한 액세스 제한 구성

**SMB** 서버에 **GPO**를 사용하기 위한 요구 사항

SMB 서버에서 GPO(그룹 정책 개체)를 사용하려면 시스템이 여러 요구 사항을 충족해야 합니다.

- SMB는 클러스터에서 라이선스가 있어야 합니다. SMB 라이선스는 에 포함되어 있습니다 ["ONTAP 1 을 참조하십시오"](#). ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.
- SMB 서버는 Windows Active Directory 도메인에 구성 및 가입해야 합니다.
- SMB 서버 관리자 상태는 켜져야 합니다.
- GPO를 구성하고 SMB 서버 컴퓨터 개체가 포함된 Windows Active Directory OU(조직 단위)에 적용해야 합니다.
- SMB 서버에서 GPO 지원을 활성화해야 합니다.

**CIFS** 서버에서 **GPO** 지원을 설정하거나 해제합니다

CIFS 서버에서 GPO(그룹 정책 개체) 지원을 설정하거나 해제할 수 있습니다. CIFS 서버에서 GPO 지원을 설정하면 CIFS 서버 컴퓨터 개체가 포함된 OU(조직 구성 단위)에 적용되는 그룹 정책에 정의된 적용 가능한 GPO가 CIFS 서버에 적용됩니다.



이 작업에 대해

워크그룹 모드에서는 CIFS 서버에서 GPO를 설정할 수 없습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
GPO를 활성화합니다	'vserver cifs group-policy modify -vserver_vserver_name_-status enabled'
GPO를 비활성화합니다	'vserver cifs group-policy modify -vserver_vserver_name_-status disabled'

2. GPO 지원이 'vserver cifs group-policy show-vserver+vserver\_name\_'(SVM CIFS 그룹 정책 표시) 상태로 설정되어 있는지 확인합니다

워크그룹 모드의 CIFS 서버에 대한 그룹 정책 상태는 "사용 안 함"으로 표시됩니다.

예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에 대한 GPO 지원을 설정합니다.

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

Vserver: vs1
Group Policy Status: enabled
```

관련 정보

지원되는 GPO

GPO를 CIFS 서버와 함께 사용하기 위한 요구 사항

CIFS 서버에서 GPO를 업데이트하는 방법

CIFS 서버에서 GPO 설정을 수동으로 업데이트합니다

GPO 구성에 대한 정보 표시

**SMB** 서버에서 **GPO**를 업데이트하는 방법

**CIFS** 서버 개요에서 **GPO**를 업데이트하는 방법

기본적으로 ONTAP는 90분마다 GPO(그룹 정책 개체) 변경 내용을 검색하고 적용합니다. 보안 설정은 16시간마다 새로 고쳐집니다. ONTAP에서 GPO를 자동으로 업데이트하기 전에 GPO를 업데이트하여 새 GPO 정책 설정을 적용하려면 ONTAP 명령을 사용하여 CIFS 서버에서 수동 업데이트를 트리거하면 됩니다.

- 기본적으로 모든 GPO는 90분마다 확인 및 업데이트됩니다.

이 간격은 구성 가능하며 '새로 고침 간격' 및 '임의 오프셋' GPO 설정을 사용하여 설정할 수 있습니다.

ONTAP는 Active Directory에 GPO 변경 사항을 쿼리합니다. Active Directory에 기록된 GPO 버전 번호가 CIFS 서버의 GPO 버전 번호보다 높을 경우 ONTAP는 새 GPO를 검색하고 적용합니다. 버전 번호가 같으면 CIFS 서버의 GPO가 업데이트되지 않습니다.

- 보안 설정 GPO는 16시간마다 새로 고쳐집니다.

ONTAP는 이러한 GPO의 변경 여부에 관계없이 보안 설정 GPO를 16시간마다 검색하고 적용합니다.



현재 ONTAP 버전에서는 16시간 기본값을 변경할 수 없습니다. Windows 클라이언트 기본 설정입니다.

- 모든 GPO는 ONTAP 명령을 사용하여 수동으로 업데이트할 수 있습니다.

이 명령은 Windows 'gpupdate.exe' /force' 명령을 시뮬레이션합니다.

## 관련 정보

### CIFS 서버에서 GPO 설정을 수동으로 업데이트합니다

#### CIFS 서버에서 GPO 설정을 수동으로 업데이트합니다

CIFS 서버에서 GPO(그룹 정책 개체) 설정을 즉시 업데이트하려면 설정을 수동으로 업데이트할 수 있습니다. 변경된 설정만 업데이트하거나 이전에 적용되었지만 변경되지 않은 설정을 포함하여 모든 설정에 대해 업데이트를 적용할 수 있습니다.

#### 단계

1. 적절한 작업을 수행합니다.

업데이트하려면...	명령 입력...
GPO 설정이 변경되었습니다	'vserver cifs group-policy update-vserver_vserver_name_'
모든 GPO 설정	'vserver cifs group-policy update-vserver_vserver_name_-force-re애플리케이션-all-settings true'

## 관련 정보

### CIFS 서버에서 GPO를 업데이트하는 방법

#### GPO 구성에 대한 정보를 표시합니다

Active Directory에 정의된 GPO(그룹 정책 개체) 구성과 CIFS 서버에 적용된 GPO 구성에 대한 정보를 표시할 수 있습니다.

#### 이 작업에 대해

CIFS 서버가 속한 도메인의 Active Directory에 정의된 모든 GPO 구성에 대한 정보를 표시하거나 CIFS 서버에 적용된 GPO 구성에 대한 정보만 표시할 수 있습니다.

#### 단계

1. 다음 작업 중 하나를 수행하여 GPO 구성에 대한 정보를 표시합니다.

모든 그룹 정책 구성에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy show-defined-vserver_vserver_name_'
CIFS 지원 스토리지 가상 시스템(SVM)에 적용	'vserver cifs group-policy show-applied-vserver_vserver_name_'

## 예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory에 정의된 GPO 구성을 보여 줍니다.



```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache : version1
```

```
Security Settings:
```

```
    Event Audit and Event Log:
```

```
        Audit Logon Events: none
```

```
        Audit Object Access: success
```

```
        Log Retention Method: overwrite-as-needed
```

```
        Max Log Size: 16384
```

```
File Security:
```

```
    /vol1/home
```

```
    /vol1/dirl
```

```
Kerberos:
```

```
    Max Clock Skew: 5
```

```
    Max Ticket Age: 10
```

```
    Max Renew Age: 7
```

```
Privilege Rights:
```

```
    Take Ownership: usr1, usr2
```

```
    Security Privilege: usr1, usr2
```

```
    Change Notify: usr1, usr2
```

```
Registry Values:
```

```
    Signing Required: false
```

```
Restrict Anonymous:
```

```
    No enumeration of SAM accounts: true
```

```
    No enumeration of SAM accounts and shares: false
```

```
    Restrict anonymous access to shares and named pipes: true
```

```
    Combined restriction for anonymous user: no-access
```

```
Restricted Groups:
```

```
    gpr1
```

```
    gpr2
```

```
Central Access Policy Settings:
```

```
    Policies: cap1
```

```
            cap2
```

```

GPO Name: Resultant Set of Policy
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication for Mode BranchCache: per-share
  Hash Version Support for BranchCache: version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

```

다음 예에서는 CIFS 지원 SVM VS1 V1에 적용된 GPO 구성을 보여 줍니다.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

Vserver: vs1

-----

GPO Name: Default Domain Policy

Level: Domain

Status: enabled

Advanced Audit Settings:

Object Access:

Central Access Policy Staging: failure

Registry Settings:

Refresh Time Interval: 22

Refresh Random Offset: 8

Hash Publication Mode for BranchCache: per-share

Hash Version Support for BranchCache: all-versions

Security Settings:

Event Audit and Event Log:

Audit Logon Events: none

Audit Object Access: success

Log Retention Method: overwrite-as-needed

Max Log Size: 16384

File Security:

/vol1/home

/vol1/dirl

Kerberos:

Max Clock Skew: 5

Max Ticket Age: 10

Max Renew Age: 7

Privilege Rights:

Take Ownership: usr1, usr2

Security Privilege: usr1, usr2

Change Notify: usr1, usr2

Registry Values:

Signing Required: false

Restrict Anonymous:

No enumeration of SAM accounts: true

No enumeration of SAM accounts and shares: false

Restrict anonymous access to shares and named pipes: true

Combined restriction for anonymous user: no-access

Restricted Groups:

gpr1

gpr2

Central Access Policy Settings:

Policies: cap1

cap2

GPO Name: Resultant Set of Policy

Level: RSOP

#### Advanced Audit Settings:

##### Object Access:

Central Access Policy Staging: failure

#### Registry Settings:

Refresh Time Interval: 22

Refresh Random Offset: 8

Hash Publication Mode for BranchCache: per-share

Hash Version Support for BranchCache: all-versions

#### Security Settings:

##### Event Audit and Event Log:

Audit Logon Events: none

Audit Object Access: success

Log Retention Method: overwrite-as-needed

Max Log Size: 16384

##### File Security:

/vol1/home

/vol1/dir1

##### Kerberos:

Max Clock Skew: 5

Max Ticket Age: 10

Max Renew Age: 7

##### Privilege Rights:

Take Ownership: usr1, usr2

Security Privilege: usr1, usr2

Change Notify: usr1, usr2

##### Registry Values:

Signing Required: false

##### Restrict Anonymous:

No enumeration of SAM accounts: true

No enumeration of SAM accounts and shares: false

Restrict anonymous access to shares and named pipes: true

Combined restriction for anonymous user: no-access

##### Restricted Groups:

gpr1

gpr2

#### Central Access Policy Settings:

Policies: cap1

cap2

#### 관련 정보

[CIFS 서버에서 GPO 지원을 설정하거나 해제합니다](#)

제한된 그룹 **GPO**에 대한 자세한 정보를 표시합니다

Active Directory에서 GPO(그룹 정책 개체)로 정의되고 CIFS 서버에 적용되는 제한된 그룹에 대한 자세한 정보를 표시할 수 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- 그룹 정책 이름입니다
- 그룹 정책 버전입니다
- 링크

그룹 정책이 구성되는 수준을 지정합니다. 가능한 출력 값은 다음과 같습니다.

- ONTAP에서 그룹 정책이 구성되면 Local이 됩니다
- 도메인 컨트롤러의 사이트 수준에서 그룹 정책이 구성되면 '사이트'입니다
- 도메인 컨트롤러의 도메인 수준에서 그룹 정책이 구성되면 "domain"입니다
- 조직 단위(OrganizationalUnit) - 도메인 컨트롤러의 조직 단위(OU) 수준에서 그룹 정책이 구성된 경우
- 다양한 수준에서 정의된 모든 그룹 정책에서 파생된 정책의 결과 집합에 대한 RSoP
- 제한된 그룹 이름입니다
- 제한된 그룹에 속하고 속하지 않는 사용자 및 그룹
- 제한된 그룹이 추가되는 그룹의 목록입니다

그룹은 여기에 나열된 그룹 이외의 그룹의 구성원이 될 수 있습니다.

단계

1. 다음 작업 중 하나를 수행하여 모든 제한된 그룹 GPO에 대한 정보를 표시합니다.

모든 제한된 그룹 <b>GPO</b> 에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy restricted-group show-defined-vserver vserver_name'
CIFS 서버에 적용됩니다	'vserver cifs group-policy restricted-group show-applied-vserver vserver_name'

예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory 도메인에 정의된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy restricted-group show-defined
-vsriver vs1
```

```
Vsriver: vs1
```

```
-----
```

```
    Group Policy Name: gp01
        Version: 16
        Link: OrganizationalUnit
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9

    Group Policy Name: Resultant Set of Policy
        Version: 0
        Link: RSOP
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9
```

다음 예에서는 CIFS 지원 SVM VS1 에 적용된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy restricted-group show-applied
-vsriver vs1
```

```
Vsriver: vs1
```

```
-----
```

```
    Group Policy Name: gp01
        Version: 16
        Link: OrganizationalUnit
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9

    Group Policy Name: Resultant Set of Policy
        Version: 0
        Link: RSOP
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9
```

관련 정보

[GPO 구성에 대한 정보 표시](#)

중앙 액세스 정책에 대한 정보를 표시합니다

Active Directory에 정의된 중앙 액세스 정책에 대한 자세한 정보를 표시할 수 있습니다. GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 정책의 이름입니다
- SID
- 설명
- 생성 시간
- 수정 시간
- 구성원 규칙



CIFS 서버는 GPO를 지원하지 않으므로 워크그룹 모드의 CIFS 서버는 표시되지 않습니다.

단계

1. 다음 작업 중 하나를 수행하여 중앙 액세스 정책에 대한 정보를 표시합니다.

모든 중앙 액세스 정책에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy central-access-policy show-defined-vserver_vserver_name_'
CIFS 서버에 적용됩니다	'vserver cifs group-policy central-access-policy show-applied-vserver_vserver_name_'

예

다음 예에서는 Active Directory에 정의된 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy central-access-policy show-defined
```

```
Vserver   Name                               SID
-----
-----
vs1       p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
    Description: policy #1
    Creation Time: Tue Oct 22 09:34:13 2013
    Modification Time: Wed Oct 23 08:59:15 2013
    Member Rules: r1

vs1       p2                               S-1-17-1885229282-1100162114-134354072-
822349040
    Description: policy #2
    Creation Time: Tue Oct 22 10:28:20 2013
    Modification Time: Thu Oct 31 10:25:32 2013
    Member Rules: r1
                r2
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy central-access-policy show-applied
```

```
Vserver   Name                               SID
-----
-----
vs1       p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
    Description: policy #1
    Creation Time: Tue Oct 22 09:34:13 2013
    Modification Time: Wed Oct 23 08:59:15 2013
    Member Rules: r1

vs1       p2                               S-1-17-1885229282-1100162114-134354072-
822349040
    Description: policy #2
    Creation Time: Tue Oct 22 10:28:20 2013
    Modification Time: Thu Oct 31 10:25:32 2013
    Member Rules: r1
                r2
```

관련 정보

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)



## GPO 구성에 대한 정보 표시

### 중앙 액세스 정책 규칙에 대한 정보 표시

중앙 액세스 정책 규칙에 대한 정보를 표시합니다

Active Directory에 정의된 중앙 액세스 정책과 연결된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 중앙 액세스 정책 GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책 규칙에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

정의되고 적용된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 규칙의 이름입니다
- 설명
- 생성 시간
- 수정 시간
- 현재 권한
- 제안된 권한
- 타겟 리소스

중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy central-access-rule show-defined-vserver vserver_name'
CIFS 서버에 적용됩니다	'vserver cifs group-policy central-access-rule show-applied-vserver vserver_name'

예

다음 예에서는 Active Directory에 정의된 중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 중앙 액세스 정책과 연결된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

## 관련 정보

[DAC\(Dynamic Access Control\)를 사용하여 파일 액세스 보안](#)

[GPO 구성에 대한 정보 표시](#)

[중앙 액세스 정책에 대한 정보 표시](#)

## SMB 서버 컴퓨터 계정 암호를 관리하는 명령입니다

암호를 변경, 재설정 및 비활성화하고 자동 업데이트 일정을 구성하기 위한 명령을 알아야 합니다. SMB 서버에서 자동으로 업데이트되도록 스케줄을 구성할 수도 있습니다.

원하는 작업	이 명령 사용...
도메인 계정 암호를 변경하거나 재설정하면 암호를 알 수 있습니다	'vserver cifs domain password change'를 선택합니다
도메인 계정 암호를 재설정하며 암호를 모르는 경우	'vserver cifs domain password reset'
자동 컴퓨터 계정 암호 변경을 위해 SMB 서버를 구성합니다	'vserver cifs domain password schedule modify -vserver vs1-is-schedule -enabled true'
SMB 서버에서 자동 컴퓨터 계정 암호 변경을 비활성화합니다	'vserver cifs domain password schedule modify -vserver vs1-is-schedule -enabled false'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

## 도메인 컨트롤러 연결을 관리합니다

검색된 서버에 대한 정보를 표시합니다

CIFS 서버에서 검색된 LDAP 서버 및 도메인 컨트롤러와 관련된 정보를 표시할 수 있습니다.

단계

1. 검색된 서버와 관련된 정보를 표시하려면 'vserver cifs domain discovered-servers show' 명령을 입력합니다

예

다음 예에서는 SVM VS1 에서 검색된 서버를 보여 줍니다.

```
cluster1::> vserver cifs domain discovered-servers show
```

Node: node1

Vserver: vs1

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

관련 정보

[서버 재설정 및 재검색](#)

## CIFS 서버를 중지 또는 시작하는 중입니다

서버를 재설정하고 재검색합니다

CIFS 서버에서 서버를 재설정하고 재검색하면 CIFS 서버가 LDAP 서버 및 도메인 컨트롤러에 대한 저장된 정보를 삭제할 수 있습니다. 서버 정보를 폐기한 후 CIFS 서버는 이러한 외부 서버에 대한 현재 정보를 다시 가져옵니다. 이 기능은 연결된 서버가 적절하게 응답하지 않는 경우에 유용할 수 있습니다.

단계

1. 'vserver cifs domain discovered - servers reset -servers -vserver \_vserver\_name\_' 명령을 입력합니다
2. 새로 재검색된 서버에 대한 정보를 표시합니다. 'vserver cifs domain discovered-servers show -vserver \_vserver\_name\_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 VS1 용 서버를 재설정하고 다시 검색합니다.

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

Node: node1

Vserver: vs1

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

관련 정보

[검색된 서버에 대한 정보 표시](#)

## CIFS 서버를 중지 또는 시작하는 중입니다

도메인 컨트롤러 검색을 관리합니다

ONTAP 9.3부터는 DC(도메인 컨트롤러)가 검색되는 기본 프로세스를 수정할 수 있습니다. 이렇게 하면 사이트 또는 기본 DC 풀로 검색을 제한할 수 있으며, 이는 환경에 따라 성능 개선을 초래할 수 있습니다.

이 작업에 대해

기본적으로 동적 검색 프로세스는 기본 DC, 로컬 사이트의 모든 DC 및 모든 원격 DC를 포함하여 사용 가능한 모든 DC를 검색합니다. 이 구성을 사용하면 특정 환경에서 인증 및 공유 액세스에 지연 시간이 발생할 수 있습니다.

사용하려는 DC 풀을 이미 결정했거나 원격 DC가 부적절하거나 액세스할 수 없는 경우 검색 방법을 변경할 수 있습니다.

ONTAP 9.3 이상 릴리즈에서는 "cifs domain discovered-servers" 명령의 discovery-mode 매개 변수를 사용하여 다음 검색 옵션 중 하나를 선택할 수 있습니다.

- 도메인의 모든 DC가 검색됩니다.
- 로컬 사이트의 DC만 검색됩니다.

를 클릭합니다 default-site 사이트 및 서비스의 사이트에 할당되지 않은 LIF와 함께 이 모드를 사용하도록 SMB 서버에 대한 매개 변수를 정의할 수 있습니다.

- 서버 검색은 수행되지 않으며, SMB 서버 구성은 기본 DC에만 의존합니다.

이 모드를 사용하려면 먼저 SMB 서버의 기본 DC를 정의해야 합니다.

#### 단계

1. 원하는 검색 옵션을 지정합니다. 'vserver cifs domain discovered-servers discovery-mode modify -vserver\_vserver\_name\_-mode{all|site|none}'

'모드' 파라미터 옵션:

- 모두

사용 가능한 모든 DC를 검색합니다(기본값).

- '사이트'입니다

사이트에 대한 DC 검색을 제한합니다.

- "없음"

검색을 수행하지 않고 기본 DC만 사용하십시오.

#### 기본 도메인 컨트롤러를 추가합니다

ONTAP는 DNS를 통해 도메인 컨트롤러를 자동으로 검색합니다. 필요에 따라 특정 도메인의 기본 도메인 컨트롤러 목록에 하나 이상의 도메인 컨트롤러를 추가할 수 있습니다.

이 작업에 대해

지정된 도메인에 대한 기본 도메인 컨트롤러 목록이 이미 있는 경우 새 목록이 기존 목록과 병합됩니다.

#### 단계

1. 기본 도메인 컨트롤러 목록에 추가하려면 + "vserver cifs domain preferred-dc add-vserver\_vserver\_name\_-domain\_domain\_name\_-preferred-dc ip\_address,...+" 명령을 입력합니다

'-vserver\_vserver\_name\_'은 SVM(Storage Virtual Machine) 이름을 지정합니다.

'-domain\_domain\_name\_'은 지정된 도메인 컨트롤러가 속한 도메인의 정규화된 Active Directory 이름을 지정합니다.

'-preferred-dc\_ip\_address\_',... 기본 설정 도메인 컨트롤러의 IP 주소를 쉼표로 구분된 목록으로 지정합니다.

예

다음 명령을 실행하면 cifs.lab.example.com 도메인에 대한 외부 액세스를 관리하기 위해 SVM VS1의 SMB 서버가 사용하는 기본 도메인 컨트롤러 목록에 도메인 컨트롤러 172.17.102.25 및 172.17.102.24가 추가됩니다.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

관련 정보

[기본 도메인 컨트롤러를 관리하는 명령입니다](#)

기본 도메인 컨트롤러를 관리하는 명령입니다

기본 도메인 컨트롤러를 추가, 표시 및 제거하는 명령을 알아야 합니다.

원하는 작업	이 명령 사용...
기본 도메인 컨트롤러를 추가합니다	'vserver cifs domain preferred-dc add'
기본 도메인 컨트롤러를 표시합니다	'vserver cifs domain preferred-dc show'
기본 도메인 컨트롤러를 제거합니다	'vserver cifs domain preferred-dc remove'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

관련 정보

[기본 도메인 컨트롤러 추가 중](#)

도메인 컨트롤러에 대한 **SMB2** 연결을 설정합니다

ONTAP 9.1부터 SMB 버전 2.0을 사용하여 도메인 컨트롤러에 연결할 수 있습니다. 도메인 컨트롤러에서 SMB 1.0을 사용하지 않도록 설정한 경우 이 작업이 필요합니다. ONTAP 9.2부터는 SMB2가 기본적으로 설정됩니다.

이 작업에 대해

'MB2-enabled-for-dc-connections' 명령 옵션을 사용하면 사용 중인 ONTAP 릴리스에 대한 시스템 기본값을 사용할 수 있습니다. ONTAP 9.1의 시스템 기본값은 SMB 1.0에 대해 사용되고 SMB 2.0에는 사용되지 않습니다. ONTAP 9.2의 시스템 기본값은 SMB 1.0에 대해 활성화되어 있고 SMB 2.0에 대해 활성화되어 있습니다. 도메인 컨트롤러가 처음에 SMB 2.0을 협상할 수 없는 경우 SMB 1.0을 사용합니다.

SMB 1.0은 ONTAP에서 도메인 컨트롤러로 비활성화할 수 있습니다. ONTAP 9.1에서 SMB 1.0을 사용하지 않도록 설정한 경우 도메인 컨트롤러와 통신하려면 SMB 2.0을 활성화해야 합니다.

자세히 알아보기:

- "활성화된 SMB 버전을 확인하는 중입니다".
- "지원되는 SMB 버전 및 기능".



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

#### 단계

1. SMB 보안 설정을 변경하기 전에 어떤 SMB 버전이 활성화되어 있는지 확인하십시오: "vserver cifs security show"
2. 목록을 아래로 스크롤하여 SMB 버전을 확인합니다.
3. 'SMB2 enabled-for-dc-connections' 옵션을 사용하여 적절한 명령을 수행합니다.

SMB2가 다음과 같은 상태가 되도록 하려면...	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-SMB2-enabled-for-dc-connections true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-SMB2-enabled-for-dc-connections false'

도메인 컨트롤러에 대한 암호화된 연결을 활성화합니다

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다.

이 작업에 대해

ONTAP는 '-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러(DC) 통신을 암호화해야 하며 기본값은 false입니다. SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다.

암호화된 DC 통신이 필요한 경우 ONTAP는 SMB3 연결만 협상하므로 '-SMB2-enabled-for-DC-connections' 옵션이 무시됩니다. DC가 SMB3 및 암호화를 지원하지 않는 경우 ONTAP가 이를 통해 연결되지 않습니다.

#### 단계

1. DC와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver\_svm\_name\_-encryption-required-for-dc-connection true'

**null** 세션을 사용하여 **Kerberos**가 아닌 환경의 스토리지에 액세스합니다

**Null** 세션을 사용하여 **Kerberos**가 아닌 환경의 스토리지에 액세스 개요

null 세션 액세스는 스토리지 시스템 데이터와 같은 네트워크 리소스 및 로컬 시스템에서 실행되는 클라이언트 기반 서비스에 대한 권한을 제공합니다. 클라이언트 프로세스가 "시스템" 계정을 사용하여 네트워크 리소스에 액세스할 때 Null 세션이 발생합니다. Null 세션 구성은 비 Kerberos 인증에만 적용됩니다.

null 세션 공유는 인증이 필요하지 않으므로 null 세션 액세스가 필요한 클라이언트의 IP 주소가 스토리지 시스템에 매핑되어야 합니다.

기본적으로 매핑되지 않은 null 세션 클라이언트는 공유 열거형과 같은 특정 ONTAP 시스템 서비스에 액세스할 수 있지만 스토리지 시스템 데이터에 액세스하지 못하도록 제한됩니다.



ONTAP는 '-restricting-anonymous' 옵션을 사용하여 Windows RestrictAnonymous 레지스트리 설정 값을 지원합니다. 이렇게 하면 매핑되지 않은 null 사용자가 시스템 리소스를 보거나 액세스할 수 있는 범위를 제어할 수 있습니다. 예를 들어 공유 열거를 사용하지 않도록 설정하고 IPC\$ 공유(숨겨진 명명된 파이프 공유)에 액세스할 수 있습니다. 'vserver cifs options modify' 및 'vserver cifs options'에 man page가 표시되어 '-restrict-anonymous' 옵션에 대한 자세한 정보를 제공합니다.

달리 구성하지 않는 한 null 세션을 통해 스토리지 시스템 액세스를 요청하는 로컬 프로세스를 실행하는 클라이언트는 ""Everyone""과 같은 제한적이지 않은 그룹의 구성원입니다. 선택한 스토리지 시스템 리소스에 대해 null 세션 액세스를 제한하려면 모든 null 세션 클라이언트가 속한 그룹을 생성해야 합니다. 이 그룹을 생성하면 스토리지 시스템 액세스를 제한하고 null 세션 클라이언트에 적용되는 스토리지 시스템 리소스 권한을 설정할 수 있습니다.

ONTAP는 'vserver name-mapping' 명령 세트에서 null 사용자 세션을 사용하여 스토리지 시스템 리소스에 액세스할 수 있는 클라이언트의 IP 주소를 지정하는 매핑 구문을 제공합니다. Null 사용자에게 대한 그룹을 생성한 후에는 null 세션에만 적용되는 스토리지 시스템 리소스 및 리소스 권한에 대한 액세스 제한을 지정할 수 있습니다. Null 사용자는 익명 로그인으로 식별됩니다. Null 사용자는 홈 디렉토리에 액세스할 수 없습니다.

매핑된 IP 주소에서 스토리지 시스템을 액세스하는 모든 null 사용자에게 매핑된 사용자 권한이 부여됩니다. null 사용자로 매핑된 스토리지 시스템에 대한 무단 액세스를 방지하려면 적절한 예방 조치를 고려하십시오. 최대한의 보호를 위해, IP 주소 "스포크"의 가능성을 제거하기 위해, 별도의 네트워크에 null 사용자 스토리지 시스템 액세스를 필요로 하는 모든 클라이언트와 스토리지 시스템을 배치하십시오.

#### 관련 정보

#### 익명 사용자에게 대한 액세스 제한 구성

**Null 사용자에게 파일 시스템 공유에 대한 액세스 권한을 부여합니다**

null 세션 클라이언트가 사용할 그룹을 할당하고 null 세션 클라이언트의 IP 주소를 기록하여 null 세션을 사용하여 데이터를 액세스할 수 있는 스토리지 시스템의 클라이언트 목록에 추가하는 방식으로 null 세션 클라이언트를 통해 스토리지 시스템 리소스에 대한 액세스를 허용할 수 있습니다.

#### 단계

1. "vserver name-mapping create" 명령을 사용하여 Null 사용자를 IP 한정자를 사용하여 유효한 Windows 사용자에게 매핑합니다.

다음 명령을 실행하면 유효한 호스트 이름이 google.com 인 user1에 null 사용자가 매핑됩니다.

```
vserver name-mapping create -direction win-unix -position 1 -pattern  
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

다음 명령을 실행하면 유효한 IP 주소가 10.238.2.54/32인 user1에 null 사용자가 매핑됩니다.



```
vserver name-mapping create -direction win-unix -position 2 -pattern  
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. 이름 매핑을 확인하려면 'vserver name-mapping show' 명령을 사용하십시오.

```
vserver name-mapping show
```

Vserver: vs1  
Direction: win-unix

Position	Hostname	IP Address/Mask	
1	-	10.72.40.83/32	Pattern: anonymous logon Replacement: user1

3. "vserver cifs options modify -win-name -for-null-user" 명령을 사용하여 null 사용자에게 Windows 구성원을 할당합니다.

이 옵션은 Null 사용자에 대해 유효한 이름 매핑이 있는 경우에만 적용할 수 있습니다.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. "vserver cifs options show" 명령을 사용하여 null 사용자가 Windows 사용자 또는 그룹에 매핑되었는지 확인합니다.

```
vserver cifs options show
```

Vserver :vs1

Map Null User to Windows User of Group: user1

## SMB 서버의 NetBIOS 별칭을 관리합니다

### SMB 서버의 NetBIOS 별칭 관리 개요

NetBIOS 별칭은 SMB 클라이언트가 SMB 서버에 연결할 때 사용할 수 있는 SMB 서버의 대체 이름입니다. SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 파일 서버의 이름에 응답하도록 할 때 유용할 수 있습니다.

SMB 서버를 생성할 때 또는 SMB 서버를 생성한 후 언제든지 NetBIOS 별칭 목록을 지정할 수 있습니다. 목록에서 NetBIOS 별칭을 언제든지 추가하거나 제거할 수 있습니다. NetBIOS 별칭 목록에 있는 이름을 사용하여 SMB 서버에 연결할 수 있습니다.

관련 정보

**NetBIOS** 별칭 목록을 **SMB** 서버에 추가합니다

SMB 클라이언트가 별칭을 사용하여 SMB 서버에 접속하도록 하려면 NetBIOS 별칭 목록을 만들거나 NetBIOS 별칭의 기존 목록에 NetBIOS 별칭을 추가할 수 있습니다.

이 작업에 대해

- NetBIOS 별칭 이름은 최대 15자까지 지정할 수 있습니다.
- SMB 서버에서 최대 200개의 NetBIOS 별칭을 구성할 수 있습니다.
- 다음 문자는 허용되지 않습니다.

@# \* ()+=+[];:",<>V?

단계

1. NetBIOS 별칭: + 'vserver cifs add-netbios-alias-vserver\_vserver\_name\_-NetBIOS-alias\_netbios\_alias,...'를 추가합니다

```
'vserver cifs add-netbios-alias-vserver vs1-netbios-alias alias_1, alias_2, alias_3'
```

- 심표로 구분된 목록을 사용하여 하나 이상의 NetBIOS 별칭을 지정할 수 있습니다.
- 지정된 NetBIOS 별칭이 기존 목록에 추가됩니다.
- 목록이 현재 비어 있는 경우 새 NetBIOS 별칭 목록이 생성됩니다.

2. NetBIOS 별칭이 올바르게 추가되었는지 확인합니다. 'vserver cifs show -vserver vserver\_name -display -netbios -aliases'

```
'vserver cifs show-vserver vs1-display-netbios-aliases'
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

관련 정보

[NetBIOS 별칭 목록에서 NetBIOS 별칭을 제거합니다](#)

[CIFS 서버에서 NetBIOS 별칭 목록을 표시합니다](#)

**NetBIOS** 별칭 목록에서 **NetBIOS** 별칭을 제거합니다

CIFS 서버에 대한 특정 NetBIOS 별칭이 필요하지 않은 경우 목록에서 해당 NetBIOS 별칭을 제거할 수 있습니다. 목록에서 모든 NetBIOS 별칭을 제거할 수도 있습니다.

이 작업에 대해

심표로 구분된 목록을 사용하여 둘 이상의 NetBIOS 별칭을 제거할 수 있습니다. '-NetBIOS-aliases' 매개 변수의

값으로 '-'를 지정하여 CIFS 서버에서 모든 NetBIOS 별칭을 제거할 수 있습니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

을(를) 제거하려면...	입력...
목록에서 특정 NetBIOS 별칭	'vserver cifs remove-netbios-alias-vserver_name_-netbios-alias_netbios_alias,...'
목록에서 모든 NetBIOS 별칭	'vserver cifs remove-netbios-aliases-vserver_vserver_name_-netbios-aliases-'

```
'vserver cifs remove-netbios-alias-vserver vs1-netbios-alias_1'
```

2. 지정된 NetBIOS 별칭이 제거되었는지 확인합니다. 'vserver cifs show -vserver\_vserver\_name\_-display-netbios-aliases'

```
'vserver cifs show-vserver vs1-display-netbios-aliases'
```

```
Vserver: vs1

Server Name: CIFS_SERVER
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

#### CIFS 서버의 NetBIOS 별칭 목록을 표시합니다

NetBIOS 별칭 목록을 표시할 수 있습니다. 이 기능은 SMB 클라이언트가 CIFS 서버에 접속할 수 있는 이름 목록을 확인하려는 경우에 유용할 수 있습니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	입력...
CIFS 서버의 NetBIOS 별칭입니다	'vserver cifs show-display-netbios-aliases'
자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록입니다	'vserver cifs show-instance'

다음 예에서는 CIFS 서버의 NetBIOS 별칭에 대한 정보를 표시합니다.

```
'vserver cifs show-display-netbios-aliases'
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

다음 예에서는 자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록을 표시합니다.

'vserver cifs show-instance'

```
Vserver: vs1
CIFS Server NetBIOS Name: CIFS_SERVER
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: ALIAS_1, ALIAS_2,
ALIAS_3
```

자세한 내용은 명령에 대한 man 페이지를 참조하십시오.

관련 정보

[CIFS 서버에 NetBIOS 별칭 목록을 추가합니다](#)

[CIFS 서버를 관리하는 명령입니다](#)

**SMB** 클라이언트가 **NetBIOS** 별칭을 사용하여 연결되어 있는지 확인합니다

SMB 클라이언트가 NetBIOS 별칭을 사용하여 연결되어 있는지 여부와 연결된 경우 연결에 사용되는 NetBIOS 별칭을 확인할 수 있습니다. 이 기능은 연결 문제를 해결할 때 유용할 수 있습니다.

이 작업에 대해

SMB 연결에 연결된 NetBIOS 별칭(있는 경우)을 표시하려면 '-instance' 매개 변수를 사용해야 합니다. CIFS 서버 이름 또는 IP 주소를 사용하여 SMB 연결을 수행하는 경우 NetBIOS 이름 필드의 출력은 "-"(하이픈)입니다.

단계

1. 원하는 작업을 수행합니다.

다음에 대한 <b>NetBIOS</b> 정보를 표시하려면...	입력...
SMB 연결	'vserver cifs session show-instance'

다음에 대한 <b>NetBIOS</b> 정보를 표시하려면...	입력...
지정된 NetBIOS 별칭을 사용하는 연결:	'vserver cifs session show-instance-netbios-name_netbios_name_'

다음 예에서는 세션 ID 1과 SMB 연결을 설정하는 데 사용되는 NetBIOS 별칭에 대한 정보를 표시합니다.

'vserver cifs session show-session-id 1-instance'

```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted

```

## 기타 **SMB** 서버 작업을 관리합니다

### **CIFS** 서버를 중지하거나 시작합니다

사용자가 SMB 공유를 통해 데이터에 액세스하지 않는 상태에서 작업을 수행할 때 유용할 수 있는 SVM에서 CIFS 서버를 중지할 수 있습니다. CIFS 서버를 시작하여 SMB 액세스를 재시작할 수 있습니다. CIFS 서버를 중지하면 스토리지 가상 시스템(SVM)에서 허용되는 프로토콜도 수정할 수 있습니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
CIFS 서버를 중지합니다	'vserver cifs stop-vserver_vserver_name_[-foreground{true
false}]'	CIFS 서버를 시작합니다
'vserver cifs start -vserver_vserver_name_[-foreground{true	false}]'

'-foreground'는 포그라운드와 배경에서 명령을 실행할지 여부를 지정합니다. 이 매개 변수를 입력하지 않으면 true로 설정되고 포그라운드에서 명령이 실행됩니다.

2. 'vserver cifs show' 명령을 사용하여 CIFS 서버 관리 상태가 올바른지 확인합니다.

예

다음 명령은 SVM VS1 에서 CIFS 서버를 시작합니다.

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

cluster1::> vserver cifs show -vserver vs1

Vserver: vs1
CIFS Server NetBIOS Name: VS1
NetBIOS Domain/Workgroup Name: DOMAIN
Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
```

관련 정보

[검색된 서버에 대한 정보 표시](#)

[서버 재설정 및 재검색](#)

**CIFS** 서버를 다른 **OU**로 이동합니다

CIFS 서버 생성 프로세스는 다른 OU를 지정하지 않는 한 설정 중에 기본 OU(조직 구성 단위) CN=컴퓨터를 사용합니다. 설정 후 CIFS 서버를 다른 OU로 이동할 수 있습니다.

단계

1. Windows 서버에서 \* Active Directory 사용자 및 컴퓨터 \* 트리를 엽니다.
2. SVM(스토리지 가상 머신)에 대한 Active Directory 개체를 찾습니다.
3. 개체를 마우스 오른쪽 단추로 클릭하고 \* 이동 \* 을 선택합니다.
4. SVM과 연결할 OU를 선택합니다

## 결과

SVM 객체가 선택한 OU에 배치됩니다.

**SMB** 서버를 이동하기 전에 **SVM**에서 동적 **DNS** 도메인을 수정합니다

SMB 서버를 다른 도메인으로 이동할 때 Active Directory 통합 DNS 서버가 DNS에 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SMB 서버를 이동하기 전에 SVM(스토리지 가상 시스템)에서 DDNS(동적 DNS)를 수정해야 합니다.

### 시작하기 전에

SMB 서버 컴퓨터 계정이 포함될 새 도메인의 서비스 위치 레코드가 포함된 DNS 도메인을 사용하려면 SVM에서 DNS 이름 서비스를 수정해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서버를 사용해야 합니다.

### 이 작업에 대해

DDNS(SVM에서 구성된 경우)는 데이터 LIF의 DNS 레코드를 자동으로 새 도메인에 추가하지만 원래 도메인의 DNS 레코드는 원래 DNS 서버에서 자동으로 삭제되지 않습니다. 수동으로 삭제해야 합니다.

SMB 서버를 이동하기 전에 DDNS 수정을 완료하려면 다음 항목을 참조하십시오.

["동적 DNS 서비스를 구성합니다"](#)

**SVM**을 **Active Directory** 도메인에 연결합니다

"vserver cifs modify" 명령을 사용하여 도메인을 수정하여 기존 SMB 서버를 삭제하지 않고 SVM(스토리지 가상 시스템)을 Active Directory 도메인에 연결할 수 있습니다. 현재 도메인에 다시 참가하거나 새 도메인에 가입할 수 있습니다.

### 시작하기 전에

- SVM에는 이미 DNS 구성이 있어야 합니다.
- SVM을 위한 DNS 구성은 타겟 도메인을 지원할 수 있어야 합니다.

DNS 서버에는 도메인 LDAP 및 도메인 컨트롤러 서버에 대한 SRV(서비스 위치 레코드)가 포함되어 있어야 합니다.

### 이 작업에 대해

- Active Directory 도메인 수정을 진행하려면 CIFS 서버의 관리 상태를 "down"으로 설정해야 합니다.
- 명령이 성공적으로 완료되면 관리 상태가 자동으로 ""설정""으로 설정됩니다.
- 도메인에 가입할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

### 단계

1. SVM을 CIFS 서버 도메인에 가입합니다. 'vserver cifs modify -vserver\_vserver\_name\_-domain\_domain\_name\_-status -admin down'

자세한 내용은 'vserver cifs modify' 명령에 대한 man 페이지를 참조하십시오. 새 도메인에 대한 DNS를 재구성해야 하는 경우 'vserver DNS modify' 명령에 대한 man 페이지를 참조하십시오.

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 'example'.com 도메인 내의 'ou=\_example\_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

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.

2. CIFS 서버가 원하는 Active Directory 도메인에 있는지 확인합니다. 'vserver cifs show'

예

다음 예에서는 SVM VS1 의 SMB 서버 ""CIFSSERVER1""이 keytab 인증을 사용하여 example.com 도메인에 연결됩니다.

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

**NetBIOS over TCP** 연결에 대한 정보를 표시합니다

NBT(NetBIOS over TCP) 연결에 대한 정보를 표시할 수 있습니다. 이는 NetBIOS 관련 문제를 해결할 때 유용할 수 있습니다.

단계

1. 'vserver cifs nbtstat' 명령을 사용하여 NetBIOS over TCP 연결에 대한 정보를 표시합니다.



IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

예

다음 예제에서는 ""cluster1""에 대해 표시되는 NetBIOS 이름 서비스 정보를 보여 줍니다.



```

cluster1::> vservice cifs nbtstat

Vservice: vs1
Node:      cluster1-01
Interfaces:
            10.10.10.32
            10.10.10.33
Servers:
            17.17.1.2  (active  )
NBT Scope:
            [ ]
NBT Mode:
            [h]
NBT Name      NetBIOS Suffix   State   Time Left   Type
-----
CLUSTER_1     00                          wins     57
CLUSTER_1     20                          wins     57

Vservice: vs1
Node:      cluster1-02
Interfaces:
            10.10.10.35
Servers:
            17.17.1.2  (active  )
CLUSTER_1     00                          wins     58
CLUSTER_1     20                          wins     58
4 entries were displayed.

```

## SMB 서버 관리를 위한 명령입니다

생성, 표시, 수정, 중지, 시작 명령을 알아야 합니다. 및 SMB 서버 삭제. 또한 서버를 재설정 및 재검색, 컴퓨터 계정 암호 변경 또는 재설정, 컴퓨터 계정 암호 변경 예약, NetBIOS 별칭 추가 또는 제거 등의 명령도 있습니다.

원하는 작업	이 명령 사용...
SMB 서버를 생성합니다	'vservice cifs create'
SMB 서버에 대한 정보를 표시합니다	'vservice cifs show'
SMB 서버를 수정합니다	'vservice cifs modify(가상 CIFS 수정)'
SMB 서버를 다른 도메인으로 이동합니다	'vservice cifs modify(가상 CIFS 수정)'

SMB 서버를 중지합니다	'vserver cifs stop'
SMB 서버를 시작합니다	'vserver cifs start'를 선택합니다
SMB 서버를 삭제합니다	'vserver cifs delete'
SMB 서버의 서버를 재설정하고 다시 검색합니다	'vserver cifs domain discovered - servers reset-servers'
SMB 서버의 컴퓨터 계정 암호를 변경합니다	'vserver cifs domain password change'를 선택합니다
SMB 서버의 컴퓨터 계정을 재설정합니다	'vserver cifs domain password change'를 선택합니다
SMB 서버의 컴퓨터 계정에 대한 자동 암호 변경을 예약합니다	'vserver cifs domain password schedule modify'를 참조하십시오
SMB 서버에 대한 NetBIOS 별칭을 추가합니다	'vserver cifs add-netbios-aliases'
SMB 서버의 NetBIOS 별칭을 제거합니다	'vserver cifs remove-netbios-aliases'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

#### 관련 정보

"SMB 서버를 삭제할 때 로컬 사용자 및 그룹이 어떻게 됩니까"

#### NetBIOS 이름 서비스를 활성화합니다

ONTAP 9부터는 NetBIOS 이름 서비스(NBNS, Windows 인터넷 이름 서비스 또는 WINS라고도 함)가 기본적으로 사용되지 않습니다. 이전에는 CIFS 지원 SVM(스토리지 가상 머신)이 네트워크에서 WINS가 활성화되었는지 여부에 관계없이 이름 등록 브로드캐스트를 전송했습니다. NBNS가 필요한 구성으로 이러한 브로드캐스트를 제한하려면 새 CIFS 서버에 대해 NBNS를 명시적으로 설정해야 합니다.

#### 시작하기 전에

- 이미 NBNS를 사용하고 있으며 ONTAP 9로 업그레이드하는 경우 이 작업을 완료할 필요가 없습니다. NBNS는 이전과 마찬가지로 계속 작동합니다.
- NBNS는 UDP(포트 137)를 통해 활성화됩니다.
- IPv6을 통한 NBNS는 지원되지 않습니다.

#### 단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

## 2. CIFS 서버에서 NBNS를 설정합니다.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled true
```

## 3. 관리자 권한 수준으로 돌아갑니다.

```
set -privilege admin
```

## SMB 액세스 및 SMB 서비스에 IPv6를 사용합니다

### IPv6을 사용하기 위한 요구 사항

SMB 서버에서 IPv6를 사용하려면 먼저 IPv6를 지원하는 ONTAP 및 SMB 버전과 라이선스 요구 사항이 무엇인지 알아야 합니다.

#### ONTAP 라이선스 요구 사항

SMB 라이선스가 있는 경우 IPv6에 대한 특수 라이선스가 필요하지 않습니다. SMB 라이선스는 에 포함되어 있습니다 ["ONTAP 1 을 참조하십시오"](#). ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

#### SMB 프로토콜 버전 요구 사항

- SVM의 경우 ONTAP는 모든 버전의 SMB 프로토콜에서 IPv6를 지원합니다.



IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

### SMB 액세스 및 CIFS 서비스를 통해 IPv6를 지원합니다

CIFS 서버에서 IPv6를 사용하려면 ONTAP가 CIFS 서비스에 대한 SMB 액세스 및 네트워크 통신을 위해 IPv6를 지원하는 방법을 알고 있어야 합니다.

#### Windows 클라이언트 및 서버 지원

ONTAP는 IPv6를 지원하는 Windows 서버 및 클라이언트를 지원합니다. 다음은 Microsoft Windows 클라이언트 및 서버 IPv6 지원에 대한 설명입니다.

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 이상에서는 DNS, LDAP, CLDAP 및 Kerberos 서비스를 포함한 SMB 파일 공유 및 Active Directory 서비스에 대해 IPv6를 지원합니다.

IPv6 주소가 구성된 경우 Windows 7 및 Windows Server 2008 이상 릴리즈에서는 Active Directory 서비스에 대해 기본적으로 IPv6를 사용합니다. IPv6 연결을 통한 NTLM 및 Kerberos 인증이 모두 지원됩니다.

ONTAP에서 지원하는 모든 Windows 클라이언트는 IPv6 주소를 사용하여 SMB 공유에 연결할 수 있습니다.

ONTAP가 지원하는 Windows 클라이언트에 대한 최신 정보는 를 참조하십시오 ["상호 운용성 매트릭스"](#).



NT 도메인은 IPv6에서 지원되지 않습니다.

#### 추가 CIFS 서비스 지원

ONTAP는 SMB 파일 공유 및 Active Directory 서비스에 대한 IPv6 지원 외에도 다음에 대한 IPv6 지원을 제공합니다.

- 오프라인 폴더, 로밍 프로필, 폴더 리디렉션 및 이전 버전을 포함한 클라이언트측 서비스입니다
- 동적 홈 디렉토리(홈 디렉토리 기능), symlink 및 Widelink, BranchCache, ODX 복사 오프로드, 자동 노드 추천 등의 서버 측 서비스 및 이전 버전
- Windows 로컬 사용자 및 그룹을 사용하여 액세스 제어 및 권한 관리, CLI를 사용한 파일 권한 및 감사 정책 설정, 보안 추적, 파일 잠금 관리, SMB 작업 모니터링 등의 파일 액세스 관리 서비스입니다
- NAS 멀티 프로토콜 감사
- FPolicy를 참조하십시오
- 지속적으로 사용 가능한 공유, Witness 프로토콜 및 원격 VSS(SMB 구성 기반 Hyper-V에 사용)

#### 네임 서비스 및 인증 서비스 지원

IPv6에서는 다음 이름 서비스와의 통신이 지원됩니다.

- 도메인 컨트롤러
- DNS 서버
- LDAP 서버
- KDC 서버
- NIS 서버

#### CIFS 서버가 IPv6를 사용하여 외부 서버에 연결하는 방법

요구 사항을 충족하는 구성을 생성하려면 CIFS 서버가 외부 서버에 연결할 때 IPv6을 사용하는 방법을 알고 있어야 합니다.

- 원본 주소 선택

외부 서버에 연결하려고 시도하면 선택한 소스 주소는 대상 주소와 같은 유형이어야 합니다. 예를 들어, IPv6 주소에 연결하는 경우 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)에는 소스 주소로 사용할 IPv6 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다. 마찬가지로, SVM을 IPv4 주소에 연결할 경우 소스 주소로 사용할 IPv4 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다.

- DNS를 사용하여 동적으로 검색된 서버의 경우 서버 검색은 다음과 같이 수행됩니다.
  - 클러스터에서 IPv6이 비활성화되어 있으면 IPv4 서버 주소만 검색됩니다.
  - 클러스터에서 IPv6이 활성화되어 있으면 IPv4 및 IPv6 서버 주소가 모두 검색됩니다. 주소가 속한 서버의 적합성과 IPv6 또는 IPv4 데이터 또는 관리 LIF의 가용성에 따라 두 유형 중 하나를 사용할 수 있습니다. 동적 서버 검색은 도메인 컨트롤러 및 LSA, NETLOGON, Kerberos 및 LDAP와 같은 관련 서비스를 검색하는 데 사용됩니다.
- DNS 서버 연결

DNS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 DNS 이름 서비스 구성에 따라 달라집니다. DNS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 DNS 이름 서비스 구성에서 IPv4 주소를 사용하여 DNS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. DNS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.

- LDAP 서버 접속 구성

LDAP 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 LDAP 클라이언트 구성에 따라 달라집니다. LDAP 클라이언트가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결됩니다. 필요한 경우 LDAP 클라이언트 구성에서 IPv4 주소를 사용하여 LDAP 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. LDAP 클라이언트 구성을 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.



LDAP 클라이언트 구성은 UNIX 사용자, 그룹 및 넷그룹 이름 서비스에 대해 LDAP를 구성할 때 사용됩니다.

- NIS 서버 접속

NIS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 NIS 이름 서비스 구성에 따라 달라집니다. NIS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 NIS 이름 서비스 구성에서 IPv4 주소를 사용하여 NIS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. NIS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.



NIS 이름 서비스는 UNIX 사용자, 그룹, 넷그룹 및 호스트 이름 객체를 저장하고 관리하는 데 사용됩니다.

#### 관련 정보

[SMB를 위한 IPv6 사용\(클러스터 관리자만 해당\)](#)

[IPv6 SMB 세션에 대한 정보 모니터링 및 표시](#)

#### **SMB용 IPv6 사용(클러스터 관리자만 해당)**

클러스터 설정 중에 IPv6 네트워크가 활성화되지 않습니다. SMB용 IPv6를 사용하려면 클러스터 설정이 완료된 후 클러스터 관리자가 IPv6을 사용하도록 설정해야 합니다. 클러스터 관리자가 IPv6을 사용하도록 설정하면 전체 클러스터에 대해 설정됩니다.

#### 단계

1. IPv6 사용:'네트워크 옵션 IPv6 수정 사용 참'을 선택합니다

클러스터에서 IPv6 사용 및 IPv6 LIF 구성에 대한 자세한 내용은 `_Network Management Guide_`를 참조하십시오.

IPv6이 활성화되었습니다. SMB 액세스를 위한 IPv6 데이터 LIF를 구성할 수 있습니다.

#### 관련 정보

[IPv6 SMB 세션에 대한 정보 모니터링 및 표시](#)

["네트워크 관리"](#)

**SMB에 대해 IPv6을 사용하지 않도록 설정합니다**

네트워크 옵션을 사용하여 클러스터에 IPv6이 설정되어 있어도 동일한 명령을 사용하여 SMB용 IPv6를 해제할 수 없습니다. 대신 ONTAP은 클러스터 관리자가 클러스터에서 마지막 IPv6 사용 인터페이스를 비활성화할 때 IPv6를 비활성화합니다. IPv6 지원 인터페이스 관리에 대해서는 클러스터 관리자와 통신해야 합니다.

클러스터에서 IPv6을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 [\\_Network Management Guide\\_](#)를 참조하십시오.

관련 정보

["네트워크 관리"](#)

**IPv6 SMB** 세션에 대한 정보를 모니터링하고 표시합니다

IPv6 네트워크를 사용하여 연결된 SMB 세션에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보는 IPv6 SMB 세션에 대한 기타 유용한 정보와 함께 IPv6를 사용하여 연결 중인 클라이언트를 확인하는 데 유용합니다.

단계

1. 원하는 작업을 수행합니다.

다음 사항을 확인할 수 있습니다.	명령 입력...
SVM(스토리지 가상 시스템)에 대한 SMB 세션은 IPv6를 사용하여 연결됩니다	'vserver cifs session show -vserver_vserver_name_-instance'
IPv6은 지정된 LIF 주소를 통해 SMB 세션에 사용됩니다	'vserver cifs session show -vserver_vserver_name_-lif-address_LIF_ip_address_-instance'  'LIF_IP_address'는 데이터 LIF의 IPv6 주소입니다.

## SMB를 사용하여 파일 액세스를 설정합니다

보안 스타일을 구성합니다

보안 스타일이 데이터 액세스에 미치는 영향

보안 스타일과 그 효과는 무엇입니까

UNIX, NTFS, 혼합 및 통합 등 네 가지 보안 유형이 있습니다. 각 보안 스타일은 데이터에 대한 사용 권한이 처리되는 방식에 다른 영향을 줍니다. 용도에 맞는 적절한 보안 스타일을 선택할 수 있도록 다양한 효과를 이해해야 합니다.

보안 스타일은 클라이언트 유형이 데이터에 액세스할 수 있거나 액세스할 수 없는 형식을 결정하지 않는다는 점을 이해하는 것이 중요합니다. 보안 스타일은 ONTAP에서 데이터 액세스를 제어하는 데 사용하는 권한 유형과 이러한 권한을 수정할 수 있는 클라이언트 유형만 결정합니다.

예를 들어, 볼륨이 UNIX 보안 스타일을 사용하는 경우에도 SMB 클라이언트는 ONTAP의 멀티 프로토콜 특성으로 인해 데이터에 액세스(적절하게 인증 및 승인)할 수 있습니다. 그러나 ONTAP에서는 UNIX 클라이언트만 기본 툴을 사용하여 수정할 수 있는 UNIX 권한을 사용합니다.

보안 스타일	사용 권한을 수정할 수 있는 클라이언트입니다	클라이언트가 사용할 수 있는 권한	결과적으로 효율적인 보안 스타일을 제공합니다	파일에 액세스할 수 있는 클라이언트입니다
Unix	NFS 를 참조하십시오	NFSv3 모드 비트	Unix	NFS 및 SMB
NFSv4.x ACL	Unix	NTFS입니다	중소기업	NTFS ACL
NTFS입니다	혼합	NFS 또는 SMB	NFSv3 모드 비트	Unix
NFSv4.x ACL	Unix	NTFS ACL	NTFS입니다	통합
NFS 또는 SMB	NFSv3 모드 비트	Unix	NFSv4.1 ACL	Unix
NTFS ACL	NTFS입니다	통합(ONTAP 9.4 및 이전 릴리즈에서 무한 확장 볼륨에만 해당)	NFS 또는 SMB	NFSv3 모드 비트
Unix	NFSv4.1 ACL			NTFS ACL

FlexVol 볼륨은 UNIX, NTFS 및 혼합 보안 스타일을 지원합니다. 보안 스타일이 혼합 또는 통합된 경우 사용자가 보안 스타일을 개별적으로 설정하므로 사용자가 마지막으로 권한을 수정한 클라이언트 유형에 따라 유효 사용 권한이 달라집니다. 권한을 수정한 마지막 클라이언트가 NFSv3 클라이언트인 경우 사용 권한은 UNIX NFSv3 모드 비트입니다. 마지막 클라이언트가 NFSv4 클라이언트인 경우 사용 권한은 NFSv4 ACL입니다. 마지막 클라이언트가 SMB 클라이언트인 경우 사용 권한은 Windows NTFS ACL입니다.

통합 보안 스타일은 ONTAP 9.5 이상 릴리스에서 더 이상 지원되지 않는 무한 볼륨에서만 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 ["FlexGroup 볼륨 관리 개요"](#).

ONTAP 9.2부터 vservers security file-directory 명령에 대한 'show-Effective-permissions' 매개 변수를 사용하면 지정된 파일 또는 폴더 경로에서 Windows 또는 UNIX 사용자에게 부여된 유효한 권한을 표시할 수 있습니다. 또한 선택적 매개 변수 '-share-name'을 사용하면 유효 공유 권한을 표시할 수 있습니다.



ONTAP는 처음에 일부 기본 파일 권한을 설정합니다. 기본적으로 UNIX, 혼합 및 통합 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 UNIX이고, 기본 보안 스타일에 의해 허용되는 대로 클라이언트에 의해 구성될 때까지 유효 사용 권한 유형은 UNIX 모드 비트(별도로 지정하지 않는 경우 0755)입니다. 기본적으로 NTFS 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 NTFS이며 ACL을 통해 모든 사람에게 모든 권한을 제공할 수 있습니다.

보안 스타일을 설정하는 위치 및 시기

보안 스타일은 FlexVol 볼륨(루트 또는 데이터 볼륨) 및 qtree에서 설정할 수 있습니다. 보안 스타일은 생성 시 수동으로 설정하거나 자동으로 상속하거나 나중에 변경할 수 있습니다.

**SVM**에 사용할 보안 유형을 결정합니다

볼륨에 사용할 보안 스타일을 결정하는 데 도움이 되도록 두 가지 요소를 고려해야 합니다. 기본

요소는 파일 시스템을 관리하는 관리자 유형입니다. 2차 요소는 볼륨의 데이터에 액세스하는 사용자 또는 서비스의 유형입니다.

볼륨에 보안 스타일을 구성할 때는 최상의 보안 스타일을 선택하고 사용 권한 관리 문제를 피하기 위해 환경의 요구 사항을 고려해야 합니다. 다음 고려 사항을 통해 결정을 내릴 수 있습니다.

보안 스타일	다음 경우에 선택...
Unix	<ul style="list-style-type: none"> <li>• 파일 시스템은 UNIX 관리자가 관리합니다.</li> <li>• 대부분의 사용자는 NFS 클라이언트입니다.</li> <li>• 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다.</li> </ul>
NTFS입니다	<ul style="list-style-type: none"> <li>• 파일 시스템은 Windows 관리자가 관리합니다.</li> <li>• 대부분의 사용자는 SMB 클라이언트입니다.</li> <li>• 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다.</li> </ul>
혼합	파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다.

보안 스타일 상속의 작동 방식

새 FlexVol 볼륨 또는 qtree를 생성할 때 보안 스타일을 지정하지 않으면 보안 스타일이 다른 방식으로 상속됩니다.

보안 스타일은 다음과 같은 방식으로 상속됩니다.

- FlexVol 볼륨은 SVM이 포함된 루트 볼륨의 보안 스타일을 상속합니다.
- qtree는 포함된 FlexVol 볼륨의 보안 스타일을 상속합니다.
- 파일 또는 디렉토리는 포함된 FlexVol 볼륨 또는 qtree의 보안 스타일을 상속합니다.

**ONTAP에서 UNIX 사용 권한을 유지하는 방법**

현재 UNIX 사용 권한이 있는 FlexVol 볼륨의 파일을 Windows 응용 프로그램에서 편집하고 저장하면 ONTAP에서 UNIX 사용 권한을 보존할 수 있습니다.

Windows 클라이언트의 응용 프로그램이 파일을 편집하고 저장할 때 파일의 보안 속성을 읽고, 새 임시 파일을 만들고, 해당 속성을 임시 파일에 적용한 다음 임시 파일에 원래 파일 이름을 지정합니다.

Windows 클라이언트가 보안 속성에 대한 쿼리를 수행할 때 UNIX 권한을 정확하게 나타내는 생성된 ACL을 받습니다. 이 생성된 ACL의 유일한 목적은 파일이 Windows 애플리케이션에 의해 업데이트되므로 파일의 UNIX 사용 권한을 보존하여 결과 파일이 동일한 UNIX 사용 권한을 갖도록 하는 것입니다. ONTAP는 생성된 ACL을 사용하여 NTFS ACL을 설정하지 않습니다.



SVM에서 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 대한 UNIX 권한을 조작하려는 경우 Windows 클라이언트의 보안 탭을 사용할 수 있습니다. 또는 Windows ACL을 쿼리하고 설정할 수 있는 응용 프로그램을 사용할 수도 있습니다.

- UNIX 사용 권한 수정

Windows 보안 탭을 사용하여 혼합 보안 스타일 볼륨 또는 qtree에 대한 UNIX 권한을 보고 변경할 수 있습니다. 기본 Windows 보안 탭을 사용하여 UNIX 권한을 변경하는 경우 변경하기 전에 먼저 편집할 기존 ACE(모드 비트를 0으로 설정)를 제거해야 합니다. 또는 고급 편집기를 사용하여 권한을 변경할 수도 있습니다.

모드 권한을 사용하는 경우 나열된 UID, GID 및 기타(컴퓨터에 계정이 있는 다른 모든 사용자)에 대한 모드 권한을 직접 변경할 수 있습니다. 예를 들어, 표시된 UID에 r-x 권한이 있는 경우 UID 권한을 rwx로 변경할 수 있습니다.

- UNIX 권한을 NTFS 권한으로 변경합니다

Windows 보안 탭을 사용하면 파일 및 폴더에 UNIX 유효 보안 스타일이 있는 혼합 보안 스타일 볼륨 또는 qtree의 UNIX 보안 개체를 Windows 보안 개체로 대체할 수 있습니다.

원하는 Windows 사용자 및 그룹 개체로 대체하려면 먼저 나열된 모든 UNIX 권한 항목을 제거해야 합니다. 그런 다음 Windows 사용자 및 그룹 개체에서 NTFS 기반 ACL을 구성할 수 있습니다. 모든 UNIX 보안 개체를 제거하고 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 Windows 사용자 및 그룹만 추가하면 파일 또는 폴더의 효과적인 보안 스타일이 UNIX에서 NTFS로 변경됩니다.

폴더에 대한 권한을 변경할 때 기본 Windows 동작은 이러한 변경 내용을 모든 하위 폴더 및 파일에 전파하는 것입니다. 따라서 보안 스타일의 변경 사항을 모든 하위 폴더, 하위 폴더 및 파일에 전파하지 않으려면 전파 선택 사항을 원하는 설정으로 변경해야 합니다.

## SVM 루트 볼륨에 보안 스타일을 구성합니다

SVM(Storage Virtual Machine) 루트 볼륨 보안 스타일을 구성하여 SVM의 루트 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

### 단계

1. 보안 스타일을 정의하려면 '-rootvolume-security-style' 매개 변수와 함께 'vserver create' 명령을 사용하십시오.

루트 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합입니다.

2. 생성한 SVM의 루트 볼륨 보안 스타일('vserver show -vserver\_vserver\_name\_')을 포함하여 구성을 표시하고 확인합니다

## FlexVol 볼륨에서 보안 스타일을 구성합니다

FlexVol 볼륨 보안 스타일을 구성하여 SVM(스토리지 가상 머신)의 FlexVol 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

### 단계

1. 다음 작업 중 하나를 수행합니다.

FlexVol 볼륨이	명령 사용...
아직 없습니다	보안 스타일을 지정하기 위해 볼륨 생성 및 '-security-style' 매개 변수를 포함합니다.
이미 있습니다	볼륨 수정, -security-style 매개 변수를 포함해서 보안 스타일을 지정합니다.

FlexVol 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합입니다.

FlexVol 볼륨을 만들 때 보안 스타일을 지정하지 않으면 볼륨은 루트 볼륨의 보안 스타일을 상속합니다.

볼륨 생성 또는 볼륨 수정 명령에 대한 자세한 내용은 을 참조하십시오 ["논리적 스토리지 관리"](#).

2. 생성한 FlexVol 볼륨의 보안 스타일을 포함하여 구성을 표시하려면 다음 명령을 입력합니다.

```
'volume show-volume volume_name-instance'
```

## Qtree에서 보안 스타일 구성

Qtree 볼륨 보안 스타일을 구성하여 Qtree에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

qtree가...	명령 사용...
아직 없습니다	볼륨 qtree create를 수행하고 보안 스타일을 지정하는 -security-style 매개 변수를 포함합니다.
이미 있습니다	볼륨 qtree 수정과 보안 유형을 지정하는 -security-style 매개 변수를 포함합니다.

qtree 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS, 혼합입니다.

Qtree를 만들 때 보안 스타일을 지정하지 않으면 기본 보안 스타일이 '혼합'으로 설정됩니다.

'볼륨 qtree 생성' 또는 '볼륨 qtree 수정' 명령에 대한 자세한 내용은 을 참조하십시오 ["논리적 스토리지 관리"](#).

2. 생성한 qtree의 보안 스타일을 포함하여 구성을 표시하려면 ' volume qtree show-qtree qtree qtree\_name-instance ' 명령을 입력합니다

## NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다

### NAS 네임스페이스에서 데이터 볼륨 생성 및 관리 개요

NAS 환경에서 파일 액세스를 관리하려면 SVM(스토리지 가상 머신)에서 데이터 볼륨과 접합

지점을 관리해야 합니다. 여기에는 네임스페이스 아키텍처 계획, 접합 지점을 사용하거나 사용하지 않는 볼륨 생성, 볼륨 마운트 또는 마운트 해제, 데이터 볼륨 및 NFS 서버 또는 CIFS 서버 네임스페이스에 대한 정보 표시 등이 포함됩니다.

지정된 교차점으로 데이터 볼륨을 생성합니다

데이터 볼륨을 생성할 때 교차점을 지정할 수 있습니다. 결과 볼륨은 교차점에 자동으로 마운트되며 NAS 액세스를 위해 즉시 구성할 수 있습니다.

시작하기 전에

볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.



다음 문자는 접합 경로에 사용할 수 없습니다. `*#"><|? \`

또한 접합 경로 길이는 255자를 초과할 수 없습니다.

단계

1. `"volume create-vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size{integer[KB|MB|GB|TB|PB]}-security-style{NTFS|UNIX|MIXED}-junction-path_junction_path_"`를 사용하여 볼륨을 생성합니다

접합 경로는 루트(/)로 시작해야 하며 디렉터리와 접합된 볼륨을 모두 포함할 수 있습니다. 접합 경로에는 볼륨의 이름을 포함할 필요가 없습니다. 접합 경로는 볼륨 이름과 무관합니다.

볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 만드는 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

교차경로는 대/소문자를 구분하지 않고 `/eng`은 `/eng`과 같습니다. CIFS 공유를 생성하는 경우 Windows는 연결 경로를 대/소문자를 구분하는 것처럼 처리합니다. 예를 들어, junction이 `/eng`인 경우 CIFS 공유의 경로는 `/eng`가 아니라 `/eng`로 시작해야 합니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 자세한 내용은 볼륨 만들기 명령에 대한 `man` 페이지를 참조하십시오.

2. 볼륨이 원하는 접합 지점 `'volume show-vserver_vserver_name_-volume_volume_name_-junction'`을 사용하여 생성되었는지 확인합니다

예

다음 예에서는 junction path `"/eng/home"`이 있는 SVM VS1 상에 `""home4""`라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

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

교차점을 지정하지 않고 데이터 볼륨을 생성합니다

교차점을 지정하지 않고 데이터 볼륨을 생성할 수 있습니다. 결과 볼륨은 자동으로 마운트되지 않으며 NAS 액세스에 대해 구성할 수 없습니다. 해당 볼륨에 대해 SMB 공유 또는 NFS 내보내기를 구성하려면 먼저 볼륨을 마운트해야 합니다.

시작하기 전에

볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.

단계

1. 다음 명령을 사용하여 접합 지점 없이 볼륨을 생성합니다. 'volume create-vserver\_name\_-volume\_volume\_name\_-aggregate\_aggregate\_name\_-size{integer[KB|MB|GB|TB|PB]} - security-style{NTFS|UNIX|MIXED}'

볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 자세한 내용은 볼륨 만들기 명령에 대한 man 페이지를 참조하십시오.

2. 볼륨이 "volume show-vserver\_name\_-volume\_volume\_name\_-junction" 접합 지점 없이 생성되었는지 확인합니다

예

다음 예에서는 교차점에 마운트되지 않은 SVM VS1 상에 "sales"라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

**NAS** 네임스페이스에서 기존 볼륨을 마운트 또는 마운트 해제합니다

SVM(스토리지 가상 시스템) 볼륨에 포함된 데이터에 대한 NAS 클라이언트 액세스를 구성하려면 먼저 NAS 네임스페이스에 볼륨을 마운트해야 합니다. 볼륨이 현재 마운트되지 않은 경우 볼륨을 연결 지점에 마운트할 수 있습니다. 볼륨을 마운트 해제할 수도 있습니다.

이 작업에 대해

볼륨을 마운트 해제하고 오프라인으로 전환하면 마운트 해제된 볼륨의 네임스페이스 내에 포함된 접합 지점의 볼륨 데이터를 비롯하여 연결 지점 내의 모든 데이터를 NAS 클라이언트에서 액세스할 수 없습니다.



볼륨에 대한 NAS 클라이언트 액세스를 중단하려면 볼륨을 마운트 해제하는 것만으로는 충분하지 않습니다. 볼륨을 오프라인으로 전환하거나 클라이언트 측 파일 핸들 캐시가 무효화되도록 다른 단계를 수행해야 합니다. 자세한 내용은 다음 기술 자료 문서를 참조하십시오. ["ONTAP의 네임스페이스에서 제거후에도 NFSv3 클라이언트가 볼륨에 계속 액세스할 수 있습니다"](#)

볼륨을 마운트 해제하고 오프라인으로 전환하면 볼륨 내의 데이터가 손실되지 않습니다. 또한 마운트 해제된 볼륨 내의 볼륨이나 디렉토리 및 연결 지점에 생성된 기존 볼륨 내보내기 정책 및 SMB 공유가 보존됩니다. 마운트 해제된 볼륨을 다시 마운트하면 NAS 클라이언트가 기존 익스포트 정책과 SMB 공유를 사용하여 볼륨 내에 포함된 데이터에 액세스할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

원하는 작업	명령 입력...
볼륨을 마운트합니다	'volume mount-vserver_svm_name_- volume_volume_name_-junction- path_junction_path_'

원하는 작업	명령 입력...
볼륨을 마운트 해제합니다	<pre>volume unmount -vserver svm_name -volume volume_name</pre> <pre>volume offline -vserver svm_name -volume volume_name</pre>

## 2. 볼륨이 원하는 마운트 상태에 있는지 확인합니다.

```
volume show -vserver svm_name -volume volume_name -fields state,junction-
path,junction-active
```

예

다음 예에서는 SVM "VS1"에 있는 "판매"라는 볼륨을 접합 지점 "/판매"에 마운트합니다.

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

vserver	volume	state	junction-path	junction-active
vs1	data	online	/data	true
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

다음 예에서는 SVM "VS1"에 있는 "데이터"라는 이름의 볼륨을 마운트 해제하고 오프라인으로 전환합니다.

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

볼륨 마운트 및 접합 지점 정보를 표시합니다

스토리지 가상 시스템(SVM)에 대해 마운트된 볼륨 및 볼륨이 마운트된 접합 지점에 대한 정보를 표시할 수 있습니다. 또한 어느 볼륨이 분기점에 마운트되지 않는지 확인할 수 있습니다. 이

정보를 사용하여 SVM 네임스페이스를 이해하고 관리할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

를 표시하려면...	명령 입력...
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 요약 정보	'volume show -vserver vserver_name-junction'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 자세한 정보	'volume show -vserver vserver_name -volume volume_name -instance'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 특정 정보	<p>a. 필요한 경우 볼륨 표시 필드? 명령을 사용하여 '-fields' 매개 변수에 대한 유효한 필드를 표시할 수 있습니다</p> <p>b. '-fields' 매개 변수를 사용하여 원하는 정보를 표시합니다. volume show -vserver vserver_name -fields fieldname,...</p>

예

다음 예는 SVM VS1 에서 마운트 및 마운트 해제된 볼륨에 대한 요약을 표시합니다.

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

다음 예는 SVM VS2 에 있는 볼륨의 지정된 필드에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume    aggregate size state  type security-style junction-path
junction-parent node
-----
vs2      data1      aggr3      2GB  online RW   unix          -          -
node3
vs2      data2      aggr3      1GB  online RW   ntfs          /data2
vs2_root node3
vs2      data2_1    aggr3      8GB  online RW   ntfs          /data2/d2_1
data2     node3
vs2      data2_2    aggr3      8GB  online RW   ntfs          /data2/d2_2
data2     node3
vs2      pubs      aggr1      1GB  online RW   unix          /publications
vs2_root node1
vs2      images    aggr3      2TB  online RW   ntfs          /images
vs2_root node3
vs2      logs      aggr1      1GB  online RW   unix          /logs
vs2_root node1
vs2      vs2_root aggr3      1GB  online RW   ntfs          /          -
node3
```

## 이름 매핑을 구성합니다

### 이름 매핑 구성 개요

ONTAP은 이름 매핑을 사용하여 CIFS ID를 UNIX ID에 매핑하고, Kerberos ID를 UNIX ID에 매핑하며, UNIX ID를 CIFS ID에 매핑합니다. 사용자 자격 증명을 얻고 NFS 클라이언트나 CIFS 클라이언트에서 연결 중인지에 관계없이 적절한 파일 액세스를 제공하려면 이 정보가 필요합니다.

이름 매핑을 사용할 필요가 없는 두 가지 예외가 있습니다.

- 순수 UNIX 환경을 구성하고 볼륨에 CIFS 액세스 또는 NTFS 보안 스타일을 사용하지 않을 계획입니다.
- 대신 사용할 기본 사용자를 구성합니다.

이 시나리오에서는 모든 개별 클라이언트 자격 증명을 매핑하지 않고 모든 클라이언트 자격 증명에 동일한 기본 사용자에게 매핑되기 때문에 이름 매핑이 필요하지 않습니다.

사용자 이름 매핑만 사용할 수 있으며 그룹에서는 사용할 수 없습니다.

그러나 개별 사용자 그룹을 특정 사용자에게 매핑할 수 있습니다. 예를 들어, 영업이라는 단어가 있는 모든 AD 사용자를 특정 UNIX 사용자 및 사용자의 UID에 매핑할 수 있습니다.



ONTAP에서 사용자에게 대한 자격 증명을 매핑해야 하는 경우 먼저 로컬 이름 매핑 데이터베이스와 LDAP 서버에서 기존 매핑을 확인합니다. SVM의 네임 서비스 구성에 따라 1개 또는 2개 모두를 검사할지 여부를 결정합니다.

- Windows에서 UNIX로의 매핑의 경우

매핑을 찾을 수 없는 경우 ONTAP는 소문자 Windows 사용자 이름이 UNIX 도메인의 유효한 사용자 이름인지 확인합니다. 이렇게 해도 문제가 해결되지 않으면 기본 UNIX 사용자를 사용합니다(구성된 경우). 기본 UNIX 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

- UNIX에서 Windows로의 매핑의 경우

매핑을 찾을 수 없는 경우 ONTAP는 SMB 도메인의 UNIX 이름과 일치하는 Windows 계정을 찾으려고 시도합니다. 이 기능이 작동하지 않으면 기본 SMB 사용자를 사용합니다(구성된 경우). 기본 CIFS 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 가져올 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

컴퓨터 계정은 기본적으로 지정된 기본 UNIX 사용자에게 매핑됩니다. 기본 UNIX 사용자를 지정하지 않으면 컴퓨터 계정 매핑이 실패합니다.

- ONTAP 9.5부터 기본 UNIX 사용자가 아닌 다른 사용자에게 시스템 계정을 매핑할 수 있습니다.
- ONTAP 9.4 이하 버전에서는 시스템 계정을 다른 사용자에게 매핑할 수 없습니다.

컴퓨터 계정에 대한 이름 매핑이 정의되어 있더라도 매핑은 무시됩니다.

다중 도메인은 **UNIX** 사용자와 **Windows** 사용자 이름 매핑을 검색합니다

ONTAP는 UNIX 사용자를 Windows 사용자에게 매핑할 때 다중 도메인 검색을 지원합니다. 일치하는 결과가 반환될 때까지 검색된 모든 신뢰할 수 있는 도메인이 대체 패턴과 일치하는 항목을 검색합니다. 또는 검색된 신뢰할 수 있는 도메인 목록 대신 사용되는 기본 신뢰할 수 있는 도메인 목록을 구성할 수 있으며 일치하는 결과가 반환될 때까지 순서대로 검색됩니다.

도메인 트러스트가 **UNIX** 사용자에게 **Windows** 사용자 이름 매핑 검색에 미치는 영향

다중 도메인 사용자 이름 매핑의 작동 방식을 이해하려면 ONTAP에서 도메인 트러스트가 작동하는 방식을 이해해야 합니다. CIFS 서버의 홈 도메인과의 Active Directory 트러스트 관계는 양방향 신뢰일 수도 있고 인바운드 트러스트 또는 아웃바운드 트러스트를 포함한 두 가지 단방향 트러스트 유형 중 하나일 수도 있습니다. 홈 도메인은 SVM의 CIFS 서버가 속하는 도메인입니다.

- 양방향 트러스트

양방향 트러스트를 사용하면 두 도메인이 서로 신뢰합니다. CIFS 서버의 홈 도메인에 다른 도메인과의 양방향 트러스트가 있는 경우 홈 도메인이 신뢰할 수 있는 도메인에 속한 사용자를 인증하고 권한을 부여할 수 있으며 그 반대의 경우도 마찬가지입니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색은 홈 도메인과 다른 도메인 간의 양방향 트러스트가 있는 도메인에서만 수행할 수 있습니다.

• \_아웃바운드 트러스트 \_

아웃바운드 트러스트를 사용하면 홈 도메인이 다른 도메인을 신뢰합니다. 이 경우 홈 도메인이 아웃바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하고 권한을 부여할 수 있습니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 아웃바운드 트러스트가 `_not_sunfre` 검색되었습니다.


• \_인바운드 신뢰 \_

인바운드 트러스트를 사용하면 다른 도메인이 CIFS 서버의 홈 도메인을 신뢰합니다. 이 경우 홈 도메인은 인바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하거나 승인할 수 없습니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 인바운드 트러스트가 `_not_sound`입니다.

이름 매핑에 대한 다중 도메인 검색을 구성하는 데 와일드카드(\*)를 사용하는 방법

다중 도메인 이름 매핑 검색은 Windows 사용자 이름의 도메인 섹션에서 와일드카드를 사용하여 쉽게 수행할 수 있습니다. 다음 표에서는 이름 매핑 항목의 도메인 부분에서 와일드카드를 사용하여 다중 도메인 검색을 사용하는 방법을 보여 줍니다.

패턴	교체	결과
루트	• \\ 관리자	UNIX 사용자 "root"는 "administrator"라는 사용자에게 매핑됩니다. "administrator"라는 이름의 첫 번째 일치하는 사용자를 찾을 때까지 모든 신뢰할 수 있는 도메인을 순서대로 검색합니다.
*	\\ * \\ *	<p>유효한 UNIX 사용자는 해당 Windows 사용자에게 매핑됩니다. 모든 신뢰할 수 있는 도메인은 해당 이름을 가진 첫 번째 일치하는 사용자를 찾을 때까지 순서대로 검색됩니다.</p> <div>  <p>패턴 \\ * \\ * 은 UNIX에서 Windows로의 이름 매핑에만 유효하며 다른 방법은 사용할 수 없습니다.</p> </div>

다중 도메인 이름 검색 수행 방법

다음 두 가지 방법 중 하나를 선택하여 다중 도메인 이름 검색에 사용되는 신뢰할 수 있는 도메인 목록을 확인할 수 있습니다.

- ONTAP에서 컴파일한 자동으로 검색된 양방향 트러스트 목록을 사용합니다

- 컴파일하는 신뢰할 수 있는 기본 도메인 목록을 사용합니다

UNIX 사용자가 사용자 이름의 도메인 섹션에 와일드카드를 사용하여 Windows 사용자에게 매핑된 경우 Windows 사용자는 다음과 같이 모든 신뢰할 수 있는 도메인에서 찾을 수 있습니다.

- 선호하는 트러스트된 도메인 목록이 구성되어 있으면 매핑된 Windows 사용자는 이 검색 목록에서만 순서대로 검색됩니다.
- 신뢰할 수 있는 도메인의 기본 설정 목록이 구성되어 있지 않으면 홈 도메인의 모든 양방향 신뢰할 수 있는 도메인에서 Windows 사용자가 표시됩니다.
- 홈 도메인에 대해 양방향으로 신뢰할 수 있는 도메인이 없는 경우 사용자는 홈 도메인에서 표시됩니다.

UNIX 사용자가 사용자 이름의 도메인 섹션이 없는 Windows 사용자에게 매핑된 경우 Windows 사용자는 홈 도메인에서 찾을 수 있습니다.

## 이름 매핑 변환 규칙

ONTAP 시스템은 각 SVM에 대해 일련의 변환 규칙을 유지합니다. 각 규칙은 A\_pattern\_과 A\_replacement\_의 두 부분으로 구성됩니다. 변환은 적절한 목록의 시작 부분에서 시작하여 첫 번째 일치 규칙을 기반으로 대체를 수행합니다. 이 패턴은 UNIX 형식의 정규식입니다. 대체는 UNIX 'ed' 프로그램과 마찬가지로 패턴에서 부분식을 나타내는 이스케이프 시퀀스를 포함하는 문자열입니다.

## 이름 매핑을 생성합니다

'vserver name-mapping create' 명령을 사용하여 이름 매핑을 생성할 수 있습니다. 이름 매핑을 사용하여 Windows 사용자가 UNIX 보안 스타일 볼륨에 액세스하고 그 반대로 액세스할 수 있습니다.

## 이 작업에 대해

각 SVM에서 ONTAP은 각 방향에 대해 최대 12,500개의 이름 매핑을 지원합니다.

## 단계

1. 이름 매핑을 작성하십시오. 'vserver name-mapping create-vserver\_vserver\_name\_-direction{KRB-UNIX|win-unix|unix-win}-position\_integer\_-pattern text-replacement\_text\_'



'-pattern' 및 '-replacement' 문은 정규식으로 공식화할 수 있습니다. 또한 '-replacement' 문을 사용하여 null 대체 문자열 ""(공백 문자)를 사용하여 사용자에게 대한 매핑을 명시적으로 거부할 수 있습니다. 자세한 내용은 'vserver name-mapping create' man 페이지를 참조하십시오.

Windows와 UNIX 간 매핑이 생성될 때 새 매핑이 생성될 때 ONTAP 시스템에 대한 열린 연결이 있는 모든 SMB 클라이언트는 로그아웃했다가 다시 로그인하여 새 매핑을 확인해야 합니다.

## 예

다음 명령을 실행하면 이름이 VS1 인 SVM에 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 UNIX에서 Windows로의 매핑입니다. 매핑은 UNIX 사용자 johnd를 Windows 사용자 ENG\JohnDoe에 매핑합니다.

```
vs1::> vsserver name-mapping create -vsserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 Windows에서 UNIX로의 매핑입니다. 여기에는 정규식이 포함됩니다. 매핑은 SVM과 연결된 LDAP 도메인의 사용자에게 도메인 ENG의 모든 CIFS 사용자를 매핑합니다.

```
vs1::> vsserver name-mapping create -vsserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 이 패턴에는 이스케이프해야 하는 Windows 사용자 이름의 요소로 ""\$가 포함됩니다. 매핑은 Windows 사용자 ENG\John\$ops를 UNIX 사용자 John\_ops에 매핑합니다.

```
vs1::> vsserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john$ops
-replacement john_ops
```

기본 사용자를 구성합니다

사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우 사용할 기본 사용자를 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 사용자를 구성하지 않아야 합니다.

이 작업에 대해

CIFS 인증의 경우 각 Windows 사용자를 개별 UNIX 사용자에게 매핑하지 않으려면 대신 기본 UNIX 사용자를 지정할 수 있습니다.

NFS 인증의 경우 각 UNIX 사용자를 개별 Windows 사용자에게 매핑하지 않으려면 대신 기본 Windows 사용자를 지정할 수 있습니다.


단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
기본 UNIX 사용자를 구성합니다	'vsserver cifs options modify-default-unix-user_user_name_'
기본 Windows 사용자를 구성합니다	'vsserver nfs modify -default-win-user_user_name_'

이름 매핑을 관리하는 명령입니다

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
이름 매핑을 생성합니다	'vserver name-mapping create'
특정 위치에 이름 매핑을 삽입합니다	'vserver name-mapping insert'
이름 매핑을 표시합니다	'vserver name-mapping show'
두 이름 매핑의 위치를 교환합니다	'vserver name-mapping swap'
 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	
이름 매핑을 수정합니다	'vserver name-mapping modify'입니다
이름 매핑을 삭제합니다	'vserver name-mapping delete'
올바른 이름 매핑을 확인합니다	'vserver security file-directory show-Effective-permissions-vserver vs1-win-user-name user1-path/-share-name SH1'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

## 다중 도메인 이름 매핑 검색을 구성합니다

다중 도메인 이름 매핑 검색을 사용하거나 사용하지 않도록 설정합니다

다중 도메인 이름 매핑 검색을 사용하면 UNIX 사용자를 Windows 사용자 이름 매핑에 구성할 때 Windows 이름의 도메인 부분에서 와일드 카드(\)를 사용할 수 있습니다. 이름의 도메인 부분에서 와일드카드()를 사용하면 ONTAP에서 CIFS 서버의 컴퓨터 계정이 포함된 도메인과 양방향 트러스트가 있는 모든 도메인을 검색할 수 있습니다.

이 작업에 대해

양방향으로 신뢰할 수 있는 모든 도메인을 검색하는 대신 선호하는 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다. 선호하는 신뢰할 수 있는 도메인 목록이 구성되면 ONTAP는 검색된 양방향으로 신뢰할 수 있는 도메인 대신 선호하는 신뢰할 수 있는 도메인 목록을 사용하여 다중 도메인 이름 매핑 검색을 수행합니다.

- 다중 도메인 이름 매핑 검색은 기본적으로 사용하도록 설정됩니다.
- 이 옵션은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

2. 다음 작업 중 하나를 수행합니다.

다중 도메인 이름 매핑 검색을 사용하려는 경우...	명령 입력...
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-trusted-domain-enum -search-enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-trusted-domain-enum -search-enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

사용 가능한 SMB 서버 옵션

신뢰할 수 있는 도메인을 다시 설정하고 다시 검색합니다

신뢰할 수 있는 모든 도메인을 강제로 다시 검색할 수 있습니다. 이 기능은 신뢰할 수 있는 도메인 서버가 제대로 응답하지 않거나 트러스트 관계가 변경된 경우에 유용할 수 있습니다. CIFS 서버의 컴퓨터 계정이 포함된 도메인인 홈 도메인과의 양방향 트러스트가 있는 도메인만 검색됩니다.

단계

1. 'vserver cifs domain trusts retrover' 명령을 사용하여 신뢰할 수 있는 도메인을 재설정하고 다시 검색합니다.

```
'vserver cifs domain r트러스트 reDiscover - vserver vs1'
```

관련 정보

검색된 신뢰할 수 있는 도메인에 대한 정보 표시

검색된 신뢰할 수 있는 도메인에 대한 정보를 표시합니다

CIFS 서버의 컴퓨터 계정이 포함된 도메인인 CIFS 서버의 홈 도메인에 대해 검색된 신뢰할 수 있는 도메인에 대한 정보를 표시할 수 있습니다. 이 기능은 검색된 신뢰할 수 있는 도메인과 검색된 신뢰할 수 있는 도메인 목록 내에서 해당 도메인의 순서가 어떻게 정렬되는지 알고 싶을 때 유용합니다.

이 작업에 대해

홈 도메인과 양방향 트러스트가 있는 도메인만 검색됩니다. 홈 도메인의 DC(도메인 컨트롤러)가 DC에서 결정한 순서대로 신뢰할 수 있는 도메인 목록을 반환하므로 목록 내의 도메인 순서를 예측할 수 없습니다. 신뢰할 수 있는 도메인 목록을 표시하여 다중 도메인 이름 매핑 검색에 대한 검색 순서를 결정할 수 있습니다.

표시된 신뢰할 수 있는 도메인 정보는 노드 및 SVM(스토리지 가상 머신)별로 그룹화됩니다.

단계

1. 'vserver cifs domain trusts show' 명령을 사용하여 검색된 신뢰할 수 있는 도메인에 대한 정보를 표시합니다.

'vserver cifs domain ships ships vs1'이 표시됩니다

```
Node: node1
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM
```

#### 관련 정보

#### 신뢰할 수 있는 도메인 재설정 및 재검색

기본 설정 신뢰할 수 있는 도메인 목록에서 신뢰할 수 있는 도메인을 추가, 제거 또는 교체합니다

SMB 서버의 기본 설정 신뢰할 수 있는 도메인 목록에서 신뢰할 수 있는 도메인을 추가하거나 제거하거나 현재 목록을 수정할 수 있습니다. 기본 설정 신뢰할 수 있는 도메인 목록을 구성하는 경우 다중 도메인 이름 매핑 검색을 수행할 때 검색된 양방향 신뢰할 수 있는 도메인 대신 이 목록이 사용됩니다.

#### 이 작업에 대해

- 기존 목록에 신뢰할 수 있는 도메인을 추가하는 경우 새 목록이 기존 목록과 병합되고 끝에 새 항목이 추가됩니다. 신뢰할 수 있는 도메인은 신뢰할 수 있는 도메인 목록에 나타나는 순서대로 검색됩니다.
- 기존 목록에서 신뢰할 수 있는 도메인을 제거하고 목록을 지정하지 않는 경우 지정된 SVM(스토리지 가상 머신)에 대한 신뢰할 수 있는 전체 도메인 목록이 제거됩니다.
- 신뢰할 수 있는 도메인의 기존 목록을 수정하면 새 목록이 기존 목록을 덮어씁니다.



선호하는 트러스트된 도메인 목록에 양방향 트러스트된 도메인만 입력해야 합니다. 기본 도메인 목록에 아웃바운드 또는 인바운드 트러스트 도메인을 입력할 수 있지만 다중 도메인 이름 매핑 검색을 수행할 때는 사용되지 않습니다. ONTAP는 단방향 도메인의 항목을 건너뛰고 목록에서 다음 양방향 신뢰할 수 있는 도메인으로 이동합니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

기본 설정 신뢰할 수 있는 도메인 목록을 사용하여 다음을 수행하려면...	명령 사용...
신뢰할 수 있는 도메인을 목록에 추가합니다	'vserver cifs domain name-mapping-search add -vserver _vserver_name_-trusted-domain FQDN,...'
목록에서 신뢰할 수 있는 도메인을 제거합니다	'vserver cifs domain name-mapping-search remove -vserver _vserver_name_-trusted-domain FQDN,...']'
기존 목록을 수정합니다	'vserver cifs domain name-mapping-search modify -vserver _vserver_name_-trusted-domain FQDN,...'

예

다음 명령을 실행하면 SVM VS1 에서 사용하는 신뢰할 수 있는 도메인 2개(cifs1.example.com 및 cifs2.example.com) 추가할 수 있습니다.

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

다음 명령을 실행하면 SVM VS1 에서 사용되는 목록에서 신뢰할 수 있는 도메인 2개가 제거됩니다.

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

다음 명령을 실행하면 SVM VS1 에서 사용하는 신뢰할 수 있는 도메인 목록이 수정됩니다. 새 목록이 원본 목록을 대체합니다.

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

관련 정보

[신뢰할 수 있는 기본 도메인 목록에 대한 정보 표시](#)

기본 설정 신뢰할 수 있는 도메인 목록에 대한 정보를 표시합니다

신뢰할 수 있는 도메인이 기본 설정된 신뢰할 수 있는 도메인 목록에 있는지, 다중 도메인 이름 매핑 검색이 설정된 경우 검색 순서에 대한 정보를 표시할 수 있습니다. 자동으로 검색된 신뢰할 수 있는 도메인 목록을 사용하는 대신 기본 설정 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.



다음에 대한 정보를 표시하려면...	명령 사용...
SVM(스토리지 가상 머신)별로 그룹화된 클러스터의 모든 기본 신뢰할 수 있는 도메인	'vserver cifs domain name-mapping-search show'
지정된 SVM에서 선호 트러스트된 도메인 모두	'vserver cifs domain name-mapping-search show -vserver_vserver_name_'

다음 명령을 실행하면 클러스터의 모든 기본 설정 신뢰할 수 있는 도메인에 대한 정보가 표시됩니다.

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
-----
vs1              CIFS1.EXAMPLE.COM
```

#### 관련 정보

[기본 설정 신뢰할 수 있는 도메인 목록에서 신뢰할 수 있는 도메인 추가, 제거 또는 대체](#)

## SMB 공유를 생성하고 구성합니다

### SMB 공유 개요 생성 및 구성

사용자와 애플리케이션이 SMB를 통해 CIFS 서버의 데이터를 액세스하려면 먼저 볼륨의 명명된 액세스 지점인 SMB 공유를 생성하고 구성해야 합니다. 공유 매개 변수를 지정하고 속성을 공유하여 공유를 사용자 지정할 수 있습니다. 언제든지 기존 공유를 수정할 수 있습니다.

SMB 공유를 생성할 때 ONTAP은 모든 사용자에게 대한 모든 권한 권한이 있는 공유에 대한 기본 ACL을 생성합니다.

SMB 공유는 스토리지 가상 머신(SVM)의 CIFS 서버에 연결됩니다. SVM이 삭제되거나 SMB 공유가 연결된 CIFS 서버가 SVM에서 삭제된 경우 SMB 공유가 삭제됩니다. SVM에서 CIFS 서버를 다시 생성하는 경우 SMB 공유를 다시 생성해야 합니다.

#### 관련 정보

[SMB를 사용하여 파일 액세스를 관리합니다](#)

["Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"](#)

[볼륨에서 SMB 파일 이름 변환에 대한 문자 매핑을 구성합니다](#)

### 기본 관리 공유는 무엇입니까

SVM(스토리지 가상 시스템)에서 CIFS 서버를 생성하면 기본 관리 공유가 자동으로 생성됩니다. 이러한 기본 공유가 무엇이고 어떻게 사용되는지 이해해야 합니다.

ONTAP은 CIFS 서버를 생성할 때 다음과 같은 기본 관리 공유를 생성합니다.



ONTAP 9.8부터 관리자\$ 공유는 기본적으로 더 이상 생성되지 않습니다.

- IPC\$
- 관리 비용(ONTAP 9.7 이하 버전에만 해당)
- c\$

\$ 문자로 끝나는 공유는 숨겨진 공유이므로 기본 관리 공유는 내 컴퓨터에서 표시되지 않지만 공유 폴더를 사용하여 볼 수 있습니다.

**IPC\$ 및 admin\$** 기본 공유가 사용되는 방법입니다

IPC\$ 및 admin\$ 공유는 ONTAP에서 사용되며 Windows 관리자가 SVM에 상주하는 데이터에 액세스하는 데 사용할 수 없습니다.

- IPC\$ 공유입니다

IPC\$ 공유는 프로그램 간 통신에 필수적인 명명된 파이프를 공유하는 리소스입니다. IPC\$ 공유는 컴퓨터의 원격 관리 및 컴퓨터의 공유 리소스를 볼 때 사용됩니다. IPC\$ 공유의 공유 설정, 공유 속성 또는 ACL은 변경할 수 없습니다. IPC\$ 공유의 이름을 바꾸거나 삭제할 수도 없습니다.

- 관리 비용 공유(ONTAP 9.7 이하만 해당)



ONTAP 9.8부터 관리자\$ 공유는 기본적으로 더 이상 생성되지 않습니다.

SVM의 원격 관리 중에 admin\$ 공유가 사용됩니다. 이 리소스의 경로는 항상 SVM 루트로 연결되는 경로입니다. admin\$ 공유에 대한 공유 설정, 공유 속성 또는 ACL은 변경할 수 없습니다. admin\$ 공유의 이름을 바꾸거나 삭제할 수도 없습니다.

**c\$** 기본 공유가 사용되는 방식

c\$ 공유는 클러스터 또는 SVM 관리자가 SVM 루트 볼륨에 액세스하고 관리하는 데 사용할 수 있는 관리 공유입니다.

c\$ 공유의 특징은 다음과 같습니다.

- 이 공유의 경로는 항상 SVM 루트 볼륨의 경로이며 수정할 수 없습니다.
- c\$ 공유의 기본 ACL은 Administrator/Full Control입니다.

이 사용자는 BUILTIN\administrator입니다. 기본적으로 BUILTIN\ 관리자는 공유에 매핑하고 매핑된 루트 디렉토리에서 파일 및 폴더를 보거나, 만들거나, 수정하거나, 삭제할 수 있습니다. 이 디렉터리의 파일과 폴더를 관리할 때는 주의해야 합니다.

- c\$ 공유의 ACL을 변경할 수 있습니다.
- c\$ 공유 설정을 변경하고 속성을 공유할 수 있습니다.
- c\$ 공유를 삭제할 수 없습니다.
- SVM 관리자는 네임스페이스 접합을 교차하여 매핑된 c\$ 공유에서 나머지 SVM 네임스페이스에 액세스할 수 있습니다.
- c\$ 공유는 Microsoft 관리 콘솔을 사용하여 액세스할 수 있습니다.

## SMB 공유 이름 지정 요구 사항

SMB 서버에서 SMB 공유를 생성할 때는 ONTAP 공유 이름 지정 요구 사항을 염두에 두어야 합니다.

ONTAP의 공유 명명 규칙은 Windows의 명명 규칙과 동일하며 다음과 같은 요구 사항을 포함합니다.

- 각 공유의 이름은 SMB 서버에 대해 고유해야 합니다.
- 공유 이름은 대/소문자를 구분하지 않습니다.
- 최대 공유 이름 길이는 80자입니다.
- 유니코드 공유 이름이 지원됩니다.
- \$ 문자로 끝나는 공유 이름은 숨겨진 공유입니다.
- ONTAP 9.7 이전 버전의 경우 admin\$, ipc\$ 및 c\$ 관리 공유가 모든 CIFS 서버에서 자동으로 생성되며 예약된 공유 이름이 됩니다. ONTAP 9.8부터는 관리자\$ 공유가 더 이상 자동으로 생성되지 않습니다.
- 공유를 생성할 때 공유 이름 ONTAP\_admin\$(를) 사용할 수 없습니다.
- 공백이 포함된 공유 이름이 지원됩니다.
  - 공유 이름의 첫 문자 또는 마지막 문자로 공백을 사용할 수 없습니다.
  - 공백이 포함된 공유 이름은 따옴표로 묶어야 합니다.



작은따옴표는 공유 이름의 일부로 간주되며 따옴표 대신 사용할 수 없습니다.

- SMB 공유의 이름을 지정할 경우 다음과 같은 특수 문자가 지원됩니다.

! @#\$%&' \_ . ( ) { }

- SMB 공유의 이름을 지정할 때 다음 특수 문자는 지원되지 않습니다.

◦ " \ : ; | < > , ? \* =

다중 프로토콜 환경에서 공유를 생성할 때 디렉토리 대/소문자 구분 요구 사항

8.3 명명 체계가 사용되는 SVM에서 공유를 생성하여 이름 간 사례만 차이가 나는 디렉토리 이름을 구별할 경우, 클라이언트가 원하는 디렉토리 경로에 연결되도록 공유 경로에 8.3 이름을 사용해야 합니다.

다음 예에서는 Linux 클라이언트에 ""testdir"" 및 ""testdir""이라는 이름의 디렉토리 두 개가 생성되었습니다. 디렉토리가 포함된 볼륨의 연결 경로는 /home입니다. 첫 번째 출력은 Linux 클라이언트에서 출력되고 두 번째 출력은 SMB 클라이언트에서 출력됩니다.

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir
```

```
Directory of Z:\
```

```
04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

두 번째 디렉토리에 공유를 생성할 때 공유 경로에 8.3 이름을 사용해야 합니다. 이 예에서 첫 번째 디렉토리의 공유 경로는 "/home/testdir"이고 두 번째 디렉토리의 공유 경로는 "/home/TESTDI~1"입니다.

## SMB 공유 속성을 사용합니다

### SMB 공유 속성 개요 사용

SMB 공유의 속성을 사용자 지정할 수 있습니다.

사용 가능한 공유 속성은 다음과 같습니다.

공유 속성	설명
oplocks	이 속성은 공유에서 클라이언트 측 캐시라고도 하는 편의적 잠금을 사용하도록 지정합니다.
"탐색 가능"	이 속성을 사용하면 Windows 클라이언트가 공유를 탐색할 수 있습니다.
'하울스냅샷'	이 속성은 클라이언트가 스냅샷 복사본을 보고 이동할 수 있도록 지정합니다.
'변상강화하는'	이 속성은 공유에서 변경 통지 요청을 지원하도록 지정합니다. SVM에서 공유하면 기본 초기 속성이 됩니다.
'attributecache'	이 속성을 사용하면 SMB 공유의 파일 속성 캐싱을 통해 속성에 더 빠르게 액세스할 수 있습니다. 기본값은 특성 캐싱을 사용하지 않는 것입니다. 이 속성은 SMB 1.0을 통해 공유에 연결하는 클라이언트가 있는 경우에만 사용해야 합니다. 클라이언트가 SMB 2.x 또는 SMB 3.0을 통해 공유에 연결하는 경우에는 이 공유 속성을 사용할 수 없습니다.

공유 속성	설명
"계속 사용할 수 있습니다.	이 속성을 사용하면 SMB 클라이언트가 지속적으로 파일을 열 수 있습니다. 이렇게 열린 파일은 페일오버 및 반환과 같은 운영 중단 이벤트로부터 보호됩니다.
브랜치캐시	이 속성은 클라이언트가 이 공유 내의 파일에 대해 BranchCache 해시를 요청할 수 있도록 공유를 지정합니다. 이 옵션은 CIFS BranchCache 구성에서 ""공유당""을 운영 모드로 지정한 경우에만 유용합니다.
'액세스 기반 열거'	이 속성은 이 공유에서 Access 기반 열거(ABE)를 사용하도록 지정합니다. 개별 사용자의 액세스 권한에 따라 사용자가 ABE로 필터링된 공유 폴더를 볼 수 있으므로 사용자에게 액세스 권한이 없는 폴더 또는 기타 공유 리소스를 표시할 수 없습니다.
네임스페이스-캐싱	이 속성은 이 공유에 연결하는 SMB 클라이언트가 CIFS 서버가 반환하는 디렉터리 열거 결과를 캐시할 수 있도록 지정함으로써 성능을 향상시킬 수 있습니다. 기본적으로 SMB 1 클라이언트는 디렉터리 열거 결과를 캐시하지 않습니다. SMB 2 및 SMB 3 클라이언트는 기본적으로 캐시 디렉터리 열거 결과를 제공하므로 이 공유 속성을 지정하면 SMB 1 클라이언트 연결에만 성능 이점이 있습니다.
'암호화-데이터'	이 속성은 이 공유에 액세스할 때 SMB 암호화를 사용하도록 지정합니다. SMB 데이터에 액세스할 때 암호화를 지원하지 않는 SMB 클라이언트는 이 공유에 액세스할 수 없습니다.

기존 **SMB** 공유에서 공유 속성을 추가하거나 제거합니다

공유 속성을 추가하거나 제거하여 기존 SMB 공유를 사용자 지정할 수 있습니다. 이 기능은 환경의 변화하는 요구 사항에 맞게 공유 구성을 변경하려는 경우에 유용합니다.

시작하기 전에

수정할 속성이 있는 공유가 있어야 합니다.

이 작업에 대해

공유 속성 추가 지침:

- 쉼표로 구분된 목록을 사용하여 하나 이상의 공유 속성을 추가할 수 있습니다.
- 이전에 지정한 공유 속성은 그대로 유지됩니다.

새로 추가된 속성은 기존 공유 속성 목록에 추가됩니다.

- 공유에 이미 적용된 공유 속성에 새 값을 지정하면 새로 지정한 값이 원래 값을 대체합니다.

- 'vserver cifs share properties add' 명령을 사용하여 공유 속성을 제거할 수 없습니다.

'vserver cifs share properties remove' 명령을 사용하여 공유 속성을 제거할 수 있습니다.

공유 속성 제거 지침:

- 심표로 구분된 목록을 사용하여 하나 이상의 공유 속성을 제거할 수 있습니다.
- 이전에 지정했지만 제거하지 않은 공유 속성은 그대로 유지됩니다.

단계

1. 적절한 명령을 입력합니다.

원하는 작업	명령 입력...
공유 속성 추가	'vserver cifs 공유 속성 add-vserver_vserver_name_-share-name_share_name_-share-properties_,...'
공유 속성을 제거합니다	'vserver CIFS 공유 속성 remove-vserver_vserver_name_-share-name_share_name_-share-properties_properties_,...'

2. 공유 속성 설정을 확인합니다. 'vserver cifs share show -vserver vserver\_name -share-name share\_name'

예

다음 명령을 실행하면 SVM VS1 에서 "shhowsnapshot" 공유 속성이 "share1"이라는 공유에 추가됩니다.

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver      Share    Path      Properties    Comment    ACL
-----
vs1          share1   /share1   oplocks       -          Everyone / Full
Control
                browsable
                changenotify
                showsnapshot
```

다음 명령을 실행하면 SVM VS1 의 "shay2"라는 공유에서 탐색 가능한 공유 속성이 제거됩니다.

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name
share2 -share-properties browsable

cluster1::> vservers cifs share show -vservers vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	share2	/share2	oplocks	-	Everyone / Full
Control			changenotify		

관련 정보

[SMB 공유를 관리하는 명령입니다](#)

**force-group** 공유 설정을 사용하여 **SMB** 사용자 액세스를 최적화합니다

ONTAP 명령줄에서 UNIX 효과적인 보안이 설정된 데이터에 대한 공유를 생성할 때 해당 공유의 SMB 사용자가 생성한 모든 파일이 UNIX 그룹 데이터베이스에서 미리 정의된 그룹이어야 하는 **\_force-group\_**이라는 동일한 그룹에 속하도록 지정할 수 있습니다. **force-group**을 사용하면 다양한 그룹에 속한 SMB 사용자가 파일에 쉽게 액세스할 수 있습니다.

강제 그룹 지정은 공유가 UNIX 또는 혼합 qtree에 있는 경우에만 의미가 있습니다. 이러한 공유의 파일에 대한 액세스는 UNIX GID가 아닌 Windows 권한에 의해 결정되므로 NTFS 볼륨이나 qtree의 공유에 대해 강제 그룹을 설정할 필요가 없습니다.

공유에 대해 **force-group**이 지정된 경우 공유의 다음 내용이 적용됩니다.

- 이 공유에 액세스하는 **force-group**의 SMB 사용자는 **force-group**의 GID로 일시적으로 변경됩니다.  
이 GID를 사용하면 주 GID 또는 UID로 정상적으로 액세스할 수 없는 이 공유의 파일에 액세스할 수 있습니다.
- SMB 사용자가 생성한 이 공유의 모든 파일은 파일 소유자의 기본 GID에 관계없이 동일한 강제 그룹에 속합니다.

SMB 사용자가 NFS에서 생성된 파일에 액세스하려고 하면 SMB 사용자의 기본 GID가 액세스 권한을 결정합니다.

**force-group**은 NFS 사용자가 이 공유의 파일에 액세스하는 방법에 영향을 주지 않습니다. NFS에서 생성된 파일은 파일 소유자로부터 GID를 가져옵니다. 액세스 권한 결정은 파일에 액세스하려는 NFS 사용자의 UID 및 기본 GID를 기반으로 합니다.

**force-group**을 사용하면 다양한 그룹에 속한 SMB 사용자가 파일에 쉽게 액세스할 수 있습니다. 예를 들어 회사 웹 페이지를 저장하고 엔지니어링 및 마케팅 부서의 사용자에게 쓰기 권한을 부여하기 위해 공유를 만들고 **""webgroup1""** 그룹에 쓰기 권한을 부여할 수 있습니다. 강제 그룹 때문에 이 공유에 있는 SMB 사용자가 만든 모든 파일은 **""webgroup1""** 그룹의 소유입니다. 또한 공유에 액세스할 때 **""webgroup1""** 그룹의 GID가 자동으로 할당됩니다. 따라서 엔지니어링 및 마케팅 부서에서 사용자의 액세스 권한을 관리할 필요 없이 모든 사용자가 이 공유에 쓸 수 있습니다.

관련 정보

[그룹 강제 공유 설정을 사용하여 SMB 공유를 생성합니다](#)

그룹 강제 공유 설정을 사용하여 **SMB** 공유를 생성합니다

UNIX 파일 보안이 설정된 볼륨 또는 Qtree에서 데이터에 액세스하는 SMB 사용자가 ONTAP 동일한 UNIX 그룹에 속한 것으로 간주하도록 하려면 force-group 공유 설정을 사용하여 SMB 공유를 생성할 수 있습니다.

#### 단계

1. SMB 공유: 'vserver cifs share create-vserver\_name\_-share-name\_share\_name\_-path path path -force -group-for-create\_unix\_group\_name\_'을 생성합니다

공유의 UNC 경로('\\\\servername\\sharename\\filepath')에 256자 이상(UNC 경로의 초기 '\\\\' 제외)이 포함되어 있으면 Windows 속성 상자의 \* 보안 \* 탭을 사용할 수 없습니다. 이것은 ONTAP 문제가 아니라 Windows 클라이언트 문제입니다. 이 문제를 방지하려면 256자를 초과하는 UNC 경로를 사용하여 공유를 생성하지 마십시오.

공유가 생성된 후 force 그룹을 제거하려면 언제든지 공유를 수정하고 빈 문자열('')을 "-force-group-for-create" 매개 변수의 값으로 지정할 수 있습니다. 공유를 수정하여 강제 그룹을 제거하는 경우 이 공유에 대한 모든 기존 연결은 이전에 설정된 강제 그룹을 기본 GID로 계속 설정합니다.

#### 예

다음 명령을 실행하면 "/Corp/CompanyInfo" 디렉토리에 웹에서 액세스할 수 있는 ""웹 페이지" 공유가 생성되며, 이 디렉토리에서 SMB 사용자가 생성한 모든 파일이 webgroup1 그룹에 할당됩니다.

```
'vserver cifs share create-vserver vs1-share-name povp-path/corp/CompanyInfo-force-group-for-create webgroup1'
```

#### 관련 정보

[force-group 공유 설정을 사용하여 SMB 사용자 액세스를 최적화합니다](#)

**MMC**를 사용하여 **SMB** 공유에 대한 정보를 봅니다

SVM에서 SMB 공유에 대한 정보를 확인하고 MMC(Microsoft Management Console)를 사용하여 일부 관리 작업을 수행할 수 있습니다. 공유를 보려면 먼저 MMC를 SVM에 연결해야 합니다.

이 작업에 대해

MMC를 사용하여 SVM에 포함된 공유에 대해 다음 작업을 수행할 수 있습니다.

- 공유 보기
- 활성 세션을 봅니다
- 열린 파일을 봅니다
- 시스템의 세션, 파일 및 트리 연결 목록을 열거합니다
- 시스템에서 열려 있는 파일을 닫습니다
- 열려 있는 세션을 닫습니다
- 공유 생성/관리





이전 기능에 의해 표시되는 뷰는 특정 노드에 한정되며 클러스터에는 해당되지 않습니다. 따라서 MMC를 사용하여 SMB 서버 호스트 이름(즉, cifs01.domain.local)에 연결하면 클러스터 내의 단일 LIF로 DNS를 설정한 방법에 따라 라우팅됩니다.

ONTAP용 MMC에서는 다음 기능이 지원되지 않습니다.

- 새 로컬 사용자/그룹을 생성합니다
- 기존 로컬 사용자/그룹 관리/보기
- 이벤트 또는 성능 로그 보기
- 스토리지
- 서비스 및 애플리케이션

작업이 지원되지 않는 경우, remote procedure call failed' 오류가 발생할 수 있습니다.

### "FAQ: ONTAP에서 Windows MMC 사용"

단계

1. Windows 서버에서 컴퓨터 관리 MMC를 열려면 \* 제어판 \* 에서 \* 관리 도구 \* > \* 컴퓨터 관리 \* 를 선택합니다.
2. 작업 \* > \* 다른 컴퓨터에 연결 \* 을 선택합니다.

컴퓨터 선택 대화 상자가 나타납니다.

3. 스토리지 시스템의 이름을 입력하거나 \* Browse \* 를 클릭하여 스토리지 시스템을 찾습니다.
4. 확인 \* 을 클릭합니다.

MMC를 SVM에 연결합니다.

5. 탐색 창에서 \* 공유 폴더 \* > \* 공유 \* 를 클릭합니다.

SVM의 공유 목록이 오른쪽 표시 창에 표시됩니다.

6. 공유의 공유 속성을 표시하려면 공유를 두 번 클릭하여 \* 속성 \* 대화 상자를 엽니다.
7. MMC를 사용하여 스토리지 시스템에 접속할 수 없는 경우 스토리지 시스템에서 다음 명령 중 하나를 사용하여 BUILTIN\Administrators 그룹 또는 BUILTIN\Power Users 그룹에 사용자를 추가할 수 있습니다.

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

**SMB** 공유를 관리하는 명령입니다

'vserver cifs share' 및 'vserver cifs share properties' 명령을 사용하여 SMB 공유를 관리할 수 있습니다.

원하는 작업	이 명령 사용...
SMB 공유를 생성합니다	'vserver cifs share create
SMB 공유를 표시합니다	'vserver cifs share show'를 선택합니다
SMB 공유를 수정합니다	'vserver cifs share modify'를 선택합니다
SMB 공유를 삭제합니다	'vserver cifs share delete
기존 공유에 공유 속성을 추가합니다	'vserver cifs share properties add'를 선택합니다
기존 공유에서 공유 속성을 제거합니다	'vserver cifs share properties remove(가상 CIFS 공유 속성 제거
공유 속성에 대한 정보를 표시합니다	'vserver cifs share properties show'를 선택합니다

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

## SMB 공유 ACL을 사용하여 파일 액세스 보호

### SMB 공유 수준 ACL 관리 지침

공유 수준 ACL을 변경하여 사용자에게 공유에 대한 액세스 권한을 더 많이 또는 덜 부여할 수 있습니다. Windows 사용자 및 그룹 또는 UNIX 사용자 및 그룹을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

공유를 생성한 후에는 기본적으로 공유 레벨 ACL이 Everyone이라는 표준 그룹에 대한 읽기 액세스를 제공합니다. ACL의 읽기 액세스는 도메인의 모든 사용자와 모든 신뢰할 수 있는 도메인의 모든 사용자가 공유에 대한 읽기 전용 액세스 권한을 가지고 있음을 의미합니다.

Windows 클라이언트 또는 ONTAP 명령줄에서 MMC(Microsoft Management Console)를 사용하여 공유 수준 ACL을 변경할 수 있습니다.

MMC를 사용할 때 다음 지침이 적용됩니다.

- 지정된 사용자 및 그룹 이름은 Windows 이름이어야 합니다.
- Windows 권한만 지정할 수 있습니다.

ONTAP 명령줄을 사용할 때 다음 지침이 적용됩니다.

- 지정된 사용자 및 그룹 이름은 Windows 이름 또는 UNIX 이름일 수 있습니다.

ACL을 생성하거나 수정할 때 사용자 및 그룹 유형을 지정하지 않으면 기본 유형은 Windows 사용자 및 그룹입니다.

- Windows 권한만 지정할 수 있습니다.

## 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.

이 작업에 대해

로컬 또는 도메인 Windows 사용자 또는 그룹 이름 또는 UNIX 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	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\user_name -permission access_right</pre>
Windows 그룹	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\group_name -permission access_right</pre>
Unix 사용자입니다	<pre>'vserver cifs share access-control create- vserver_name_-share_share_name_-user-group- type_unix-user_-or-group_unix_user_name_- permission access_right'</pre>
Unix 그룹	<pre>'vserver cifs share access-control create- vserver_name_-share_share_name_-user-group- type_unix-group_-user-or- group_unix_group_name_-permission access_right'</pre>

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

예

다음 명령을 실행하면 이 표시됩니다 Change "vs1.example.com" SVM에서 "Sales" 공유를 위한 "Sales Team" Windows 그룹에 대한 권한:

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

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

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 명령을 실행하면 이 표시됩니다 Read "vs2.example.com" SVM에서 "엔지니어링" UNIX 그룹의 "ENG" 공유에 대한 승인:

```
cluster1::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs2.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs2.example.com	eng	engineering	unix-group	Read

다음 명령은 을 제공합니다 Change 호랑이 팀(Tiger Team)이라는 이름의 현지 Windows 그룹에 대한 허가 및 Full\_Control VS1 SVM의 "다타볼5" 공유에 대한 로컬 Windows 사용자의 "스UE CHANG"에 대한 권한:

```

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	Tiger Team	windows	Change
vs1	datavol5	Sue Chang	windows	Full_Control

**SMB** 공유 액세스 제어 목록을 관리하는 명령입니다

SMB ACL(액세스 제어 목록)을 관리하기 위한 명령을 알아야 합니다. 여기에는 ACL 생성, 표시, 수정 및 삭제가 포함됩니다.

원하는 작업	이 명령 사용...
새 ACL을 생성합니다	'vsserver cifs share access-control create'
ACL을 표시합니다	'vsserver cifs share access-control show'를 참조하십시오
ACL을 수정합니다	'vsserver cifs share access-control modify'를 참조하십시오
ACL을 삭제한다	'vsserver cifs share access-control delete'

파일 권한을 사용하여 파일 액세스를 보호합니다

**Windows** 보안 탭을 사용하여 고급 **NTFS** 파일 권한을 구성합니다

Windows 속성 창의 \* Windows 보안 \* 탭을 사용하여 파일 및 폴더에 대한 표준 NTFS 파일 권한을 구성할 수 있습니다.

시작하기 전에

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

이 작업에 대해

NTFS 파일 사용 권한 구성은 NTFS 보안 설명자와 연결된 NTFS DACL(임의 액세스 제어 목록)에 항목을 추가하여 Windows 호스트에서 수행됩니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다. 이러한 작업은 Windows GUI에서 자동으로 처리됩니다.

단계

1. Windows 탐색기의 \* Tools \* 메뉴에서 \* Map network drive \* 를 선택합니다.

2. 네트워크 드라이브 연결 \* 대화 상자를 완료합니다.

a. 드라이브 \* 문자를 선택합니다.

b. 폴더 \* 상자에 사용 권한을 적용할 데이터와 공유 이름을 포함하는 공유가 포함된 CIFS 서버 이름을 입력합니다.

CIFS 서버 이름이 ""cifs\_server""이고 공유 이름이 "share1"인 경우 "\\cifs\_server\share1"을 입력해야 합니다.



CIFS 서버 이름 대신 CIFS 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.

3. NTFS 파일 권한을 설정할 파일 또는 디렉터리를 선택합니다.

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

5. 보안 \* 탭을 선택합니다.

보안\* 탭에는 NTFS 권한이 설정된 사용자 및 그룹 목록이 표시됩니다. [사용 권한] 상자에 선택한 각 사용자 또는 그룹에 대해 적용되는 허용 및 거부 권한 목록이 표시됩니다.

6. 고급 \* 을 클릭합니다.

Windows 속성 창에는 사용자 및 그룹에 할당된 기존 파일 권한에 대한 정보가 표시됩니다.

7. 권한 변경 \* 을 클릭합니다.

사용 권한 창이 열립니다.

8. 원하는 작업을 수행합니다.

원하는 작업	다음을 수행합니다.
새 사용자 또는 그룹에 대한 고급 NTFS 권한을 설정합니다	<p>a. 추가 * 를 클릭합니다.</p> <p>b. 선택할 개체 이름 입력 * 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다.</p> <p>c. 확인 * 을 클릭합니다.</p>

원하는 작업	다음을 수행합니다.
사용자 또는 그룹의 고급 NTFS 권한을 변경합니다	a. 사용 권한 항목: * 상자에서 고급 사용 권한을 변경할 사용자 또는 그룹을 선택합니다. b. 편집 * 을 클릭합니다.
사용자 또는 그룹에 대한 고급 NTFS 권한을 제거합니다	a. 사용 권한 항목: * 상자에서 제거할 사용자 또는 그룹을 선택합니다. b. 제거 * 를 클릭합니다. c. 13단계로 건너뛵니다.

새 사용자 또는 그룹에 고급 NTFS 권한을 추가하거나 기존 사용자 또는 그룹에 대한 NTFS 고급 권한을 변경하는 경우 <Object>의 권한 항목 상자가 열립니다.

9. 적용 대상 \* 상자에서 이 NTFS 파일 권한 항목을 적용할 방법을 선택합니다.

단일 파일에 NTFS 파일 권한을 설정하는 경우 \* 적용 대상 \* 상자가 활성화되지 않습니다. 적용 대상 \* 설정은 기본적으로 \* 이 개체만 \* 으로 설정됩니다.

10. 사용 권한 \* 상자에서 이 개체에 설정할 고급 권한에 대해 \* 허용 \* 또는 \* 거부 \* 상자를 선택합니다.

- 지정된 액세스를 허용하려면 \* 허용 \* 상자를 선택합니다.
- 지정된 액세스를 허용하지 않으려면 \* Deny \* 상자를 선택합니다. 다음과 같은 고급 권한에 대한 권한을 설정할 수 있습니다.
- \* 완전 제어 \*

이 고급 권한을 선택하면 다른 모든 고급 권한이 자동으로 선택됩니다(권한 허용 또는 거부).

- \* 폴더 트래버스/파일 실행 \*
- \* 폴더 나열/데이터 읽기 \*
- \* 읽기 속성 \*
- \* 확장 속성 읽기 \*
- \* 파일 생성/데이터 쓰기 \*
- \* 폴더 생성/데이터 추가 \*
- \* 속성 쓰기 \*
- \* 확장 속성 쓰기 \*
- \* 하위 폴더 및 파일 삭제 \*
- \* 삭제 \*
- \* 읽기 권한 \*
- \* 권한 변경 \*
- \* 소유권 가져오기 \*



고급 사용 권한 상자 중 하나를 선택할 수 없는 경우 상위 개체에서 사용 권한이 상속되기 때문입니다.

11. 이 개체의 하위 폴더와 파일이 이러한 권한을 상속하도록 하려면 \* 이 컨테이너 내의 개체 및/또는 컨테이너에 이 권한을 적용합니다 \* 상자를 선택합니다.

12. 확인 \* 을 클릭합니다.

13. NTFS 사용 권한 추가, 제거 또는 편집을 마친 후 이 개체에 대한 상속 설정을 지정합니다.

- 이 개체의 부모 \* 상자에서 상속 가능한 사용 권한 포함 을 선택합니다.

이것이 기본값입니다.

- 모든 자식 개체 권한을 이 개체의 상속 가능한 권한으로 바꾸기 \* 상자를 선택합니다.

단일 파일에 NTFS 파일 권한을 설정하는 경우 사용 권한 상자에 이 설정이 없습니다.



이 설정을 선택할 때는 주의하십시오. 이 설정은 모든 자식 개체에 대한 기존 사용 권한을 모두 제거하고 이 개체의 사용 권한 설정으로 바꿉니다. 제거하지 않으려는 사용 권한을 실수로 제거할 수 있습니다. 혼합 보안 형식 볼륨 또는 qtree에서 사용 권한을 설정할 때는 특히 중요합니다. 자식 개체에 UNIX 효과적인 보안 스타일이 있는 경우 이러한 자식 개체에 NTFS 권한을 전파하면 ONTAP에서 이러한 개체를 UNIX 보안 스타일에서 NTFS 보안 스타일로 변경하고 해당 자식 개체에 대한 모든 UNIX 권한이 NTFS 권한으로 대체됩니다.

- 두 상자를 모두 선택합니다.
- 어느 상자도 선택하지 않습니다.

14. 확인 \* 을 클릭하여 \* 권한 \* 상자를 닫습니다.

15. [확인]을 클릭하여 <개체>\* 상자의 \* 고급 보안 설정을 닫습니다.

고급 NTFS 권한을 설정하는 방법에 대한 자세한 내용은 Windows 설명서를 참조하십시오.

## 관련 정보

[CLI를 사용하여 NTFS 파일 및 폴더에 파일 보안을 구성하고 적용합니다](#)

[NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보 표시](#)

[혼합 보안 형식 볼륨의 파일 보안에 대한 정보 표시](#)

[UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보 표시](#)

**ONTAP CLI를 사용하여 NTFS 파일 권한을 구성합니다**

ONTAP CLI를 사용하여 파일 및 디렉토리에 대한 NTFS 파일 권한을 구성할 수 있습니다. 따라서 Windows 클라이언트에서 SMB 공유를 사용하여 데이터에 연결할 필요 없이 NTFS 파일 권한을 구성할 수 있습니다.

NTFS 보안 설명자와 연결된 NTFS DACL(임의 액세스 제어 목록)에 항목을 추가하여 NTFS 파일 권한을 구성할 수 있습니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉토리에 적용됩니다.



명령줄을 사용해서만 NTFS 파일 권한을 구성할 수 있습니다. CLI를 사용하여 NFSv4 ACL을 구성할 수 없습니다.

단계

1. NTFS 보안 설명자를 만듭니다.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. NTFS 보안 설명자에 DACL을 추가합니다.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. 파일/디렉토리 보안 정책을 생성합니다.

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

**UNIX** 파일 권한이 **SMB**를 통해 파일에 액세스할 때 액세스 제어를 제공하는 방법

FlexVol 볼륨은 NTFS, UNIX 또는 MIXED의 세 가지 보안 유형 중 하나를 가질 수 있습니다. 보안 스타일에 관계없이 SMB를 통해 데이터에 액세스할 수 있지만 UNIX의 효율적인 보안을 통해 데이터에 액세스하려면 적절한 UNIX 파일 권한이 필요합니다.

SMB를 통해 데이터에 액세스할 때 사용자가 요청된 작업을 수행할 수 있는 권한이 있는지 여부를 결정할 때 여러 액세스 제어가 사용됩니다.

- 권한 내보내기

SMB 액세스에 대한 내보내기 권한 구성은 선택 사항입니다.

- 공유 권한
- 파일 권한

사용자가 작업을 수행하려는 데이터에 다음 유형의 파일 권한이 적용될 수 있습니다.

- NTFS입니다
- Unix NFSv4 ACL
- UNIX 모드 비트

NFSv4 ACL 또는 UNIX 모드 비트 세트가 있는 데이터의 경우 데이터에 대한 파일 액세스 권한을 결정하는 데 UNIX 스타일 권한이 사용됩니다. SVM 관리자는 사용자가 원하는 작업을 수행할 권한을 갖도록 적절한 파일 권한을 설정해야 합니다.



혼합 보안 형식 볼륨의 데이터는 NTFS 또는 UNIX의 효과적인 보안 스타일을 가질 수 있습니다. 데이터에 UNIX 유효 보안 스타일이 있는 경우 데이터에 대한 파일 액세스 권한을 결정할 때 NFSv4 사용 권한 또는 UNIX 모드 비트가 사용됩니다.

## DAC(Dynamic Access Control)를 사용하여 파일 액세스 보안

### DAC(Dynamic Access Control) 개요를 사용하여 파일 액세스 보호

동적 액세스 제어를 사용하고 Active Directory에서 중앙 액세스 정책을 생성한 후 적용된 GPO(그룹 정책 개체)를 통해 SVM의 파일 및 폴더에 적용하여 액세스를 보호할 수 있습니다. 중앙 액세스 정책 스테이징 이벤트를 사용하여 변경 내용을 적용하기 전에 중앙 액세스 정책에 대한 영향을 확인할 수 있도록 감사를 구성할 수 있습니다.

#### CIFS 자격 증명에 추가

동적 액세스 제어 전에 CIFS 자격 증명에는 보안 주체(사용자의) ID와 Windows 그룹 구성원이 포함되어 있습니다. 동적 액세스 제어를 사용하면 디바이스 ID, 디바이스 클레임 및 사용자 클레임을 비롯한 세 가지 유형의 정보가 자격 증명에 추가됩니다.

- 장치 ID

사용자가 로그인하는 장치의 ID 및 그룹 멤버십은 제외하고 사용자의 ID 정보의 아날로그.

- 장치 요청

장치 보안 주체에 대한 어설션. 예를 들어 장치 클레임은 특정 OU의 구성원일 수 있습니다.

- 사용자 클레임

사용자 보안 주체에 대한 어설션. 예를 들어 사용자 클레임은 AD 계정이 특정 OU의 구성원일 수 있습니다.

#### 중앙 액세스 정책

파일에 대한 중앙 액세스 정책을 사용하면 조직에서 사용자 그룹, 사용자 클레임, 장치 클레임 및 리소스 속성을 사용하는 조건부 식을 포함하는 인증 정책을 중앙에서 배포하고 관리할 수 있습니다.

예를 들어, 비즈니스에 큰 영향을 미치는 데이터에 액세스하려면 정규직 직원이어야 하며 관리되는 장치의 데이터만 액세스할 수 있어야 합니다. 중앙 액세스 정책은 Active Directory에서 정의되고 GPO 메커니즘을 통해 파일 서버로 배포됩니다.

#### 고급 감사를 통한 중앙 액세스 정책 스테이징

중앙 액세스 정책은 '성질'일 수 있으며, 이 경우 파일 액세스 검사 중에 "what-if" 방식으로 평가됩니다. 정책이 적용된 경우 어떤 결과가 발생했는지, 현재 구성된 것과 어떻게 다른 결과가 감사 이벤트로 기록됩니다. 이렇게 하면 관리자가 감사 이벤트 로그를 사용하여 실제로 정책을 적용하기 전에 액세스 정책 변경의 영향을 확인할 수 있습니다. 액세스 정책 변경의 영향을 평가한 후 GPO를 통해 원하는 SVM에 정책을 배포할 수 있습니다.

#### 관련 정보

[지원되는 GPO](#)

CIFS 서버에 그룹 정책 객체 적용

CIFS 서버에서 GPO 지원을 설정하거나 해제합니다

GPO 구성에 대한 정보 표시

중앙 액세스 정책에 대한 정보 표시

중앙 액세스 정책 규칙에 대한 정보 표시

CIFS 서버의 데이터를 보호하기 위해 중앙 액세스 정책 구성

동적 액세스 제어 보안에 대한 정보 표시

"SMB 및 NFS 감사 및 보안 추적"

지원되는 동적 액세스 제어 기능

CIFS 서버에서 DAC(동적 액세스 제어)를 사용하려면 ONTAP가 Active Directory 환경에서 동적 액세스 제어 기능을 지원하는 방법을 이해해야 합니다.

동적 액세스 제어에 지원됩니다

ONTAP는 CIFS 서버에서 동적 액세스 제어가 설정된 경우 다음 기능을 지원합니다.

기능	설명
파일 시스템에 대한 클레임입니다	청구는 사용자에게 대한 일부 진실을 나타내는 간단한 이름 및 값 쌍입니다. 사용자 자격 증명에는 클레임 정보가 포함되며 파일의 보안 설명자는 클레임 검사가 포함된 액세스 검사를 수행할 수 있습니다. 따라서 관리자는 파일에 액세스할 수 있는 사용자를 보다 세밀하게 제어할 수 있습니다.
파일 액세스 검사에 대한 조건식입니다	파일의 보안 매개 변수를 수정할 때 사용자는 임의로 복잡한 조건식을 파일의 보안 설명자에 추가할 수 있습니다. 조건부 표현식에는 클레임 확인이 포함될 수 있습니다.
중앙 액세스 정책을 통해 파일 액세스를 중앙 집중식으로 제어	중앙 액세스 정책은 파일에 태그를 지정할 수 있는 Active Directory에 저장된 일종의 ACL입니다. 디스크에 있는 보안 설명자와 태그가 지정된 중앙 액세스 정책 모두의 액세스 검사가 액세스를 허용하는 경우에만 파일에 대한 액세스가 부여됩니다. 따라서 관리자는 디스크의 보안 설명자를 수정하지 않고도 중앙 위치(AD)에서 파일에 대한 액세스를 제어할 수 있습니다.
중앙 액세스 정책 스테이징	중앙 액세스 정책의 "변경"을 통해 실제 파일 액세스에 영향을 주지 않고 보안 변경 사항을 시도하는 기능을 추가하고 감사 보고서에서 변경 효과를 확인할 수 있습니다.

기능	설명
ONTAP CLI를 사용하여 중앙 액세스 정책 보안에 대한 정보 표시 지원	'vserver security file-directory show' 명령을 확장하여 적용된 중앙 액세스 정책에 대한 정보를 표시합니다.
중앙 액세스 정책을 포함하는 보안 추적	적용된 중앙 액세스 정책에 대한 정보가 포함된 결과를 표시하도록 'vserver security trace' 명령 제품군을 확장합니다.

동적 액세스 제어에 지원되지 않습니다

CIFS 서버에서 동적 액세스 제어가 설정된 경우 ONTAP는 다음 기능을 지원하지 않습니다.

기능	설명
NTFS 파일 시스템 객체의 자동 분류	이 확장명은 ONTAP에서 지원되지 않는 Windows 파일 분류 인프라스트럭처의 확장입니다.
중앙 액세스 정책 스테이징 이외의 고급 감사	고급 감사를 위해 중앙 액세스 정책 스테이징만 지원됩니다.

**CIFS** 서버에서 동적 액세스 제어 및 중앙 액세스 정책을 사용할 때의 고려 사항

DAC(Dynamic Access Control) 및 중앙 액세스 정책을 사용하여 CIFS 서버의 파일과 폴더를 보호할 때 고려해야 할 몇 가지 사항이 있습니다.

정책 규칙이 **DOMAIN\administrator** 사용자에게 적용되는 경우 **NFS** 액세스가 루트에 대해 거부될 수 있습니다

특정 상황에서는 루트 사용자가 액세스하려는 데이터에 중앙 액세스 정책 보안이 적용될 때 루트에 대한 NFS 액세스가 거부될 수 있습니다. 이 문제는 중앙 액세스 정책에 도메인\관리자에게 적용되는 규칙이 포함되어 있고 루트 계정이 도메인\관리자 계정에 매핑된 경우에 발생합니다.

도메인\관리자 사용자에게 규칙을 적용하는 대신 도메인\관리자 그룹과 같은 관리 권한이 있는 그룹에 규칙을 적용해야 합니다. 이렇게 하면 이 문제의 근본 영향을 받지 않고 root를 domain\administrator 계정에 매핑할 수 있습니다.

**Active Directory**에서 적용된 중앙 액세스 정책을 찾을 수 없는 경우 **CIFS** 서버의 **BUILTIN\Administrators** 그룹에 리소스에 대한 액세스 권한이 있습니다

CIFS 서버에 포함된 리소스에 중앙 액세스 정책이 적용될 수 있지만 CIFS 서버가 중앙 액세스 정책의 SID를 사용하여 Active Directory에서 정보를 검색하려고 하면 SID가 Active Directory의 기존 중앙 액세스 정책 SID와 일치하지 않습니다. 이러한 경우 CIFS 서버는 해당 리소스에 대한 로컬 기본 복구 정책을 적용합니다.

로컬 기본 복구 정책을 사용하면 CIFS 서버의 BUILTIN\Administrators 그룹이 해당 리소스에 액세스할 수 있습니다.

동적 액세스 제어 개요 활성화 또는 비활성화

DAC(Dynamic Access Control)를 사용하여 CIFS 서버의 객체를 보호할 수 있는 옵션은 기본적으로 해제되어 있습니다. CIFS 서버에서 동적 액세스 제어를 사용하려면 이 옵션을 설정해야 합니다. 나중에 동적 액세스 제어를 사용하여 CIFS 서버에 저장된 객체를 보호하지

않으려는 경우 이 옵션을 해제할 수 있습니다.

이 작업에 대해

동적 액세스 제어 설정이 파일 시스템에 동적 액세스 제어 관련 항목이 있는 ACL이 포함될 수 있습니다. 동적 액세스 제어를 사용하지 않으면 현재 동적 액세스 제어 항목은 무시되고 새 항목은 허용되지 않습니다.

이 옵션은 고급 권한 수준에서만 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced: 'Set-Privilege advanced'로 설정합니다.
2. 다음 작업 중 하나를 수행합니다.

동적 액세스 제어를 원하는 경우...	명령 입력...
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-dac-enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-dac-enabled false'

3. 관리자 권한 수준으로 복귀: 'Set-Privilege admin'

관련 정보

[CIFS 서버의 데이터를 보호하기 위해 중앙 액세스 정책 구성](#)

동적 액세스 제어를 사용하지 않도록 설정한 경우 동적 액세스 제어 **ACE**를 포함하는 **ACL**을 관리합니다

동적 액세스 제어 ACE로 ACL이 적용된 리소스가 있고 SVM(스토리지 가상 시스템)에서 동적 액세스 제어를 사용하지 않도록 설정한 경우 해당 리소스에서 비 동적 액세스 제어 ACE를 관리하기 전에 동적 액세스 제어 ACE를 제거해야 합니다.

이 작업에 대해

동적 액세스 제어를 사용하지 않도록 설정한 후에는 기존 동적 액세스 제어 ACE를 제거하거나 기존 동적 액세스 제어 ACE를 제거해야 새로운 비 동적 액세스 제어 ACE를 추가할 수 있습니다.

일반적으로 ACL을 관리하는 데 사용하는 툴을 사용하여 이러한 단계를 수행할 수 있습니다.

단계

1. 리소스에 적용되는 동적 액세스 제어 ACE를 결정합니다.
2. 리소스에서 동적 액세스 제어 ACE를 제거합니다.
3. 리소스에서 원하는 대로 비 동적 액세스 제어 ACE를 추가하거나 제거합니다.

**CIFS** 서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다

CIFS 서버에서 DAC(Dynamic Access Control) 활성화, Active Directory에서 중앙 액세스 정책 구성, GPO를 사용하여 Active Directory 컨테이너에 중앙 액세스 정책 적용 등 중앙 액세스 정책을 사용하여 CIFS 서버의 데이터에 안전하게 액세스하기 위해 수행해야 하는 몇 가지 단계가

있습니다. 그리고 CIFS 서버에서 GPO를 사용하도록 설정합니다.

시작하기 전에

- 중앙 액세스 정책을 사용하도록 Active Directory를 구성해야 합니다.
- 중앙 액세스 정책을 만들고 CIFS 서버가 포함된 컨테이너에 GPO를 만들고 적용하려면 Active Directory 도메인 컨트롤러에 대한 충분한 액세스 권한이 있어야 합니다.
- 필요한 명령을 실행하려면 SVM(스토리지 가상 머신)에 대한 충분한 관리 액세스 권한이 있어야 합니다.

이 작업에 대해

중앙 액세스 정책은 Active Directory의 GPO(그룹 정책 개체)에 정의되고 적용됩니다. 중앙 액세스 정책 및 GPO 구성에 대한 지침은 Microsoft TechNet 라이브러리를 참조하십시오.

["Microsoft TechNet 라이브러리"](#)

단계

1. "vserver cifs options modify" 명령을 사용하여 아직 활성화되지 않은 SVM에서 동적 액세스 제어를 활성화하십시오.

```
'vserver cifs options modify -vserver vs1-is-dac-enabled true'
```

2. "vserver cifs group-policy modify" 명령을 사용하여 CIFS 서버가 아직 설정되지 않은 경우 CIFS 서버에서 GPO(그룹 정책 개체)를 사용하도록 설정합니다.

```
'vserver cifs group-policy modify - vserver vs1-status enabled'
```

3. Active Directory에 중앙 액세스 규칙 및 중앙 액세스 정책을 생성합니다.
4. GPO(그룹 정책 개체)를 만들어 Active Directory에 중앙 액세스 정책을 배포합니다.
5. CIFS 서버 컴퓨터 계정이 있는 컨테이너에 GPO를 적용합니다.
6. 'vserver cifs group-policy update' 명령을 사용하여 CIFS 서버에 적용된 GPO를 수동으로 업데이트합니다.

```
'vserver cifs group-policy update-vserver vs1'을 선택합니다
```

7. "vserver cifs group-policy show-applied" 명령을 사용하여 GPO 중앙 액세스 정책이 CIFS 서버의 리소스에 적용되는지 확인합니다.

다음 예에서는 기본 도메인 정책에 CIFS 서버에 적용되는 두 가지 중앙 액세스 정책이 있음을 보여 줍니다.

```
'vserver cifs group-policy show-applied'
```

```
Vserver: vs1
-----
      GPO Name: Default Domain Policy
        Level: Domain
      Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
```

```
Refresh Time Interval: 22
Refresh Random Offset: 8
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dirl
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

  GPO Name: Resultant Set of Policy
  Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
```

```
Event Audit and Event Log:
  Audit Logon Events: none
  Audit Object Access: success
  Log Retention Method: overwrite-as-needed
  Max Log Size: 16384
File Security:
  /vol1/home
  /vol1/dir1
Kerberos:
  Max Clock Skew: 5
  Max Ticket Age: 10
  Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
  gpr1
  gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2
2 entries were displayed.
```

관련 정보

[GPO 구성에 대한 정보 표시](#)

[중앙 액세스 정책에 대한 정보 표시](#)

[중앙 액세스 정책 규칙에 대한 정보 표시](#)

[동적 액세스 제어 활성화 또는 비활성화](#)

동적 액세스 제어 보안에 대한 정보를 표시합니다

DAC(Dynamic Access Control) 보안에 대한 정보를 NTFS 볼륨과 NTFS 유효 보안 데이터가 혼합된 보안 스타일 볼륨에서 표시할 수 있습니다. 여기에는 조건부 ACE, 리소스 ACE 및 중앙 액세스 정책 ACE에 대한 정보가 포함됩니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.



이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'
여기서 출력은 그룹 및 사용자 SID와 함께 표시됩니다	'vserver security file-directory show -vserver vserver_name -path path -lookup-names false'
16진수 비트 마스크가 텍스트 형식으로 변환되는 파일과 디렉토리의 파일 및 디렉터리 보안에 대해 설명합니다	'vserver security file-directory show -vserver vserver_name -path path path -텍스트 마스크 true'

예

다음 예제는 SVM VS1 경로의 동적 액세스 제어 보안 정보 /vol1 을 보여줍니다.

```

cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
      Vserver: vs1
      File Path: /vol1
      File Inode Number: 112
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attribute: -
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xbf14
            Owner:CIFS1\Administrator
            Group:CIFS1\Domain Admins
            SACL - ACEs
                  ALL-Everyone-0xf01ff-OI|CI|SA|FA
                  RESOURCE ATTRIBUTE-Everyone-0x0

      ("Department_MS",TS,0x10020,"Finance")
      POLICY ID-All resources - No Write-
      0x0-OI|CI
      DACL - ACEs
            ALLOW-CIFS1\Administrator-0x1f01ff-
      OI|CI
            ALLOW-Everyone-0x1f01ff-OI|CI
            ALLOW CALLBACK-DAC\user1-0x1200a9-
      OI|CI

      ((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
      evice.department==@Resource.Department_MS)

```

## 관련 정보

[GPO 구성에 대한 정보 표시](#)

[중앙 액세스 정책에 대한 정보 표시](#)

[중앙 액세스 정책 규칙에 대한 정보 표시](#)

[동적 액세스 제어에 대한 복원 고려 사항](#)

DAC(동적 액세스 제어)를 지원하지 않는 ONTAP 버전으로 되돌릴 경우 어떤 일이 발생할지, 되돌리기 전과 후에 무엇을 해야 하는지 알고 있어야 합니다.

하나 이상의 SVM(스토리지 가상 머신)에서 동적 액세스 제어와 동적 액세스 제어를 지원하지 않는 ONTAP 버전으로 클러스터를 되돌리려면 되돌리기 전에 다음을 수행해야 합니다.

- 클러스터에서 활성화된 모든 SVM에서 동적 액세스 제어를 해제해야 합니다.
- "file-op" 이벤트 유형만 사용하려면 "cap-staging" 이벤트 유형이 포함된 클러스터의 감사 구성을 수정해야 합니다.

동적 액세스 제어 ACE가 있는 파일 및 폴더에 대한 몇 가지 중요한 복원 고려 사항을 이해하고 이에 대한 조치를 취해야 합니다.

- 클러스터를 되돌린 경우 기존 동적 액세스 제어 ACE는 제거되지 않지만 파일 액세스 검사에서는 무시됩니다.
- 동적 액세스 제어 ACE는 재버전 후에 무시되므로 동적 액세스 제어 ACE가 있는 파일에서 파일에 대한 액세스가 변경됩니다.

이렇게 하면 사용자가 이전에는 액세스할 수 없었던 파일에 액세스하거나 이전에 액세스할 수 없었던 파일에 액세스할 수 있습니다.

- 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용하여 이전 보안 수준을 복원해야 합니다.

되돌리기 전에 또는 다시 버전이 완료된 직후 작업을 수행할 수 있습니다.



동적 액세스 제어 ACE는 다시 버전 변경 후 무시되므로 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용할 때 제거할 필요가 없습니다. 그러나 필요한 경우 수동으로 제거할 수 있습니다.

동적 액세스 제어 및 중앙 액세스 정책을 구성하고 사용하는 방법에 대한 추가 정보를 찾을 수 있는 위치

동적 액세스 제어 및 중앙 액세스 정책을 구성하고 사용하는 데 도움이 되는 추가 리소스를 사용할 수 있습니다.

Active Directory에서 동적 액세스 제어 및 중앙 액세스 정책을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

["Microsoft TechNet: 동적 액세스 제어 시나리오 개요"](#)

["Microsoft TechNet: 중앙 액세스 정책 시나리오"](#)

다음 참조는 동적 액세스 제어 및 중앙 액세스 정책을 사용하고 지원하도록 SMB 서버를 구성하는 데 도움이 됩니다.

- \* SMB 서버의 GPO 사용 \*

[SMB 서버에 그룹 정책 개체 적용](#)

- \* SMB 서버에서 NAS 감사 구성 \*

["SMB 및 NFS 감사 및 보안 추적"](#)

내보내기 정책을 사용하여 **SMB** 액세스를 보호합니다

SMB 서버에서 SMB 액세스에 대한 익스포트 정책을 사용하는 경우, SMB 클라이언트에서 SVM 볼륨에 대한 액세스를 제어할 때 익스포트 정책이 사용됩니다. 데이터에 액세스하려면 SMB 액세스를 허용하는 익스포트 정책을 생성한 다음, SMB 공유를 포함하는 볼륨과 정책을 연결할 수 있습니다.

내보내기 정책에는 데이터에 대한 액세스가 허용되는 클라이언트와 읽기 전용 및 읽기-쓰기 액세스에 지원되는 인증 프로토콜을 지정하는 하나 이상의 규칙이 적용됩니다. 모든 클라이언트, 클라이언트 서브넷 또는 특정 클라이언트에 대한 SMB 액세스를 허용하고 Kerberos 인증, NTLM 인증 또는 데이터에 대한 읽기 전용 및 읽기-쓰기 액세스를 결정할 때 Kerberos 및 NTLM 인증을 사용하여 인증을 허용하도록 내보내기 정책을 구성할 수 있습니다.

내보내기 정책에 적용된 모든 내보내기 규칙을 처리한 후 ONTAP는 클라이언트에 액세스 권한이 부여되었는지 여부와 허용되는 액세스 수준을 결정할 수 있습니다. 내보내기 규칙은 Windows 사용자 및 그룹이 아니라 클라이언트 컴퓨터에 적용됩니다. 내보내기 규칙은 Windows 사용자 및 그룹 기반 인증 및 권한 부여를 대체하지 않습니다. 내보내기 규칙은 공유 및 파일 액세스 권한 외에도 액세스 보안의 또 다른 계층을 제공합니다.

볼륨에 대한 클라이언트 액세스를 구성하기 위해 각 볼륨에 정확히 하나의 익스포트 정책을 연결합니다. 각 SVM에는 여러 익스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨이 있는 SVM에 대해 다음을 수행할 수 있습니다.

- SVM의 각 볼륨에 서로 다른 익스포트 정책을 지정하여 개별 클라이언트 액세스 제어를 SVM의 각 볼륨에 할당
- 각 볼륨에 대해 새로운 익스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨에 동일한 익스포트 정책을 할당합니다.

각 SVM에는 규칙이 없는 "기본값"이라는 익스포트 정책이 하나 이상 있습니다. 이 익스포트 정책을 삭제할 수는 없지만 이름을 바꾸거나 수정할 수는 있습니다. 기본적으로 SVM의 각 볼륨은 기본 익스포트 정책과 연결됩니다. SVM에서 SMB 액세스에 대한 익스포트 정책을 사용하지 않도록 설정한 경우, "기본값" 익스포트 정책은 SMB 액세스에 영향을 미치지 않습니다.

NFS 및 SMB 호스트 모두에 대한 액세스를 제공하는 규칙을 구성하고 이 규칙을 익스포트 정책에 연결할 수 있습니다. 그런 다음, NFS 및 SMB 호스트 모두에 액세스해야 하는 데이터가 포함된 볼륨에 연결할 수 있습니다. 또는 SMB 클라이언트만 액세스해야 하는 일부 볼륨이 있는 경우, SMB 프로토콜을 사용해서만 액세스를 허용하고 읽기 전용 및 쓰기 액세스에 Kerberos 또는 NTLM(또는 둘 다)만 사용하는 규칙을 사용하여 익스포트 정책을 구성할 수 있습니다. 그러면 익스포트 정책이 SMB 액세스만 원하는 볼륨에 연결됩니다.

SMB에 대한 익스포트 정책이 설정되어 있고 클라이언트가 해당 익스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우, 요청이 실패하고 권한 거부 메시지가 표시됩니다. 클라이언트가 볼륨의 익스포트 정책에 있는 규칙과 일치하지 않으면 액세스가 거부됩니다. 내보내기 정책이 비어 있으면 모든 액세스가 암시적으로 거부됩니다. 공유 및 파일 권한이 액세스를 허용하는 경우에도 마찬가지입니다. 즉, SMB 공유가 포함된 볼륨에서 다음을 최소한으로 허용하도록 익스포트 정책을 구성해야 합니다.

- 모든 클라이언트 또는 적절한 클라이언트 하위 집합에 대한 액세스를 허용합니다
- SMB를 통한 액세스를 허용합니다
- Kerberos 또는 NTLM 인증(또는 둘 다)을 사용하여 적절한 읽기 전용 및 쓰기 액세스 허용

에 대해 자세히 알아보십시오 ["엑스포트 정책 구성 및 관리"](#).

엑스포트 규칙의 작동 방식

내보내기 규칙은 익스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을

처리하는 방법을 결정하기 위해 구성된 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청을 일치시킵니다.

클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 익스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 익스포트 정책에 표시되는 순서대로 처리됩니다. 규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 권한이 사용되며 추가 규칙은 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

다음 조건을 사용하여 내보내기 규칙을 구성하여 클라이언트 액세스 권한을 결정할 수 있습니다.

- NFSv4 또는 SMB와 같이 요청을 보내는 클라이언트에서 사용하는 파일 액세스 프로토콜입니다.
- 호스트 이름 또는 IP 주소와 같은 클라이언트 식별자입니다.
- '-clientmatch' 필드의 최대 크기는 4096자입니다.
- Kerberos v5, NTLM 또는 AUTH\_SYS와 같이 클라이언트에서 인증하는 데 사용되는 보안 유형입니다.

규칙이 여러 조건을 지정하는 경우 클라이언트는 규칙을 적용하기 위해 모든 조건을 충족해야 합니다.

예

익스포트 정책에는 다음 매개 변수가 있는 익스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0"'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv3 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.17.37입니다.

클라이언트 액세스 프로토콜이 일치하더라도 클라이언트의 IP 주소는 내보내기 규칙에 지정된 IP 주소와 다른 서브넷에 있습니다. 따라서 클라이언트 일치가 실패하고 이 규칙은 이 클라이언트에 적용되지 않습니다.

예

익스포트 정책에는 다음 매개 변수가 있는 익스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS
- '-clientmatch "10.1.16.0/255.255.255.0"'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv4 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.16.54입니다.

클라이언트 액세스 프로토콜이 일치하고 클라이언트의 IP 주소가 지정된 서브넷에 있습니다. 따라서 클라이언트 일치가 성공하고 이 규칙이 이 클라이언트에 적용됩니다. 클라이언트는 보안 유형에 관계없이 읽기-쓰기 액세스를 받습니다.

예

익스포트 정책에는 다음 매개 변수가 있는 익스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH\_SYS로 인증됩니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 따라서 두 클라이언트 모두 읽기 전용 액세스 권한이 부여됩니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

**SMB**를 통한 액세스를 제한하거나 허용하는 익스포트 정책 규칙의 예

이 예에서는 SMB 액세스에 대한 익스포트 정책이 설정된 SVM에서 SMB를 통한 액세스를 제한 또는 허용하는 익스포트 정책 규칙을 생성하는 방법을 보여줍니다.

SMB 액세스에 대한 익스포트 정책은 기본적으로 비활성화되어 있습니다. SMB 액세스에 대한 익스포트 정책을 설정한 경우에만 SMB 액세스를 제한하거나 허용하는 익스포트 정책 규칙을 구성해야 합니다.

**SMB** 액세스에 대한 익스포트 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 익스포트 규칙이 생성됩니다.

- 정책 이름: cifs1
- 색인 번호: 1
- 클라이언트 일치: 192.168.1.0/24 네트워크의 클라이언트만 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다
- 읽기 전용 액세스: NTLM 또는 Kerberos 인증을 사용하는 클라이언트에 대한 액세스
- 읽기-쓰기 액세스: Kerberos 인증을 사용하는 클라이언트에 대한 액세스

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

**SMB** 및 **NFS** 액세스에 대한 익스포트 규칙

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 익스포트 규칙이 생성됩니다.

- 정책 이름: cifs nfs1
- 색인 번호: 2

- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 및 NFS 액세스
- 읽기 전용 액세스: 모든 클라이언트에 대해
- 읽기-쓰기 액세스: Kerberos(NFS 및 SMB) 또는 NTLM 인증(SMB)을 사용하는 클라이언트에 대한 액세스
- UNIX 사용자 ID 0(영)에 대한 매핑: 사용자 ID 65534에 매핑됨(일반적으로 사용자 이름에 매핑되지 않음)
- SUID 및 SGID 액세스: 허용

```
cluster1::> vservers export-policy rule create -vservers vs1 -policyname
cifs nfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

**NTLM**을 사용한 **SMB** 액세스에 대한 내보내기 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 익스포트 규칙이 생성됩니다.

- 정책 이름: ntlm1
- 색인 번호: 1
- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다
- 읽기 전용 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다
- 읽기-쓰기 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다



NTLM 전용 액세스에 대해 읽기 전용 옵션 또는 읽기/쓰기 옵션을 구성하는 경우 클라이언트 일치 옵션에서 IP 주소 기반 항목을 사용해야 합니다. 그렇지 않으면 "액세스 거부" 오류가 발생합니다. 이는 ONTAP가 호스트 이름을 사용하여 클라이언트의 액세스 권한을 확인할 때 Kerberos SPN(서비스 사용자 이름)을 사용하기 때문입니다. NTLM 인증은 SPN 이름을 지원하지 않습니다.

```
cluster1::> vservers export-policy rule create -vservers vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

**SMB** 액세스에 대한 익스포트 정책을 설정하거나 해제합니다

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 익스포트 정책을 설정하거나 해제할 수 있습니다. 내보내기 정책을 사용하여 리소스에 대한 SMB 액세스를 제어하는 것은 선택 사항입니다.

시작하기 전에

다음은 SMB에 대한 익스포트 정책을 설정하기 위한 요구 사항입니다.

- 클라이언트에 대한 내보내기 규칙을 만들기 전에 클라이언트가 DNS에 ""PTR"" 레코드를 가지고 있어야 합니다.

- SVM이 NFS 클라이언트에 대한 액세스를 제공하고 NFS 액세스에 사용할 호스트 이름이 CIFS 서버 이름과 다른 경우 호스트 이름에 대한 ""a" 및 ""PTR"" 레코드 세트가 추가로 필요합니다.

이 작업에 대해

SVM에서 새 CIFS 서버를 설정할 때 SMB 액세스에 대한 익스포트 정책을 사용하는 것은 기본적으로 해제되어 있습니다. 인증 프로토콜 또는 클라이언트 IP 주소 또는 호스트 이름을 기반으로 액세스를 제어하려는 경우 SMB 액세스에 대한 익스포트 정책을 설정할 수 있습니다. 언제든지 SMB 액세스에 대한 익스포트 정책을 설정하거나 해제할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 익스포트 정책 활성화 또는 비활성화:
  - 내보내기 정책 활성화: 'vserver cifs options modify -vserver\_vserver\_name\_-is-exportpolicy -enabled true'
  - 익스포트 정책 비활성화: 'vserver cifs options modify -vserver\_vserver\_name\_-is-exportpolicy -enabled false'
3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 익스포트 정책을 사용하여 SVM VS1 기반 리소스에 대한 SMB 클라이언트 액세스를 제어할 수 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

## Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

기본 파일 수준 및 내보내기/공유 보안을 사용하여 액세스를 보호하는 것 외에도 ONTAP가 볼륨 수준에서 적용한 세 번째 보안 계층인 스토리지 수준 액세스 가드를 구성할 수 있습니다.

Storage-Level Access Guard는 모든 NAS 프로토콜에서 해당 프로토콜이 적용된 스토리지 객체에 액세스하는 데 적용됩니다.

NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에게 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.



## Storage-Level Access Guard 동작

- Storage-Level Access Guard는 스토리지 개체의 모든 파일 또는 모든 디렉토리에 적용됩니다.

볼륨의 모든 파일 또는 디렉토리에는 Storage-Level Access Guard 설정이 적용되기 때문에 전파를 통한 상속은 필요하지 않습니다.

- 저장소 수준 액세스 가드를 구성하여 파일에만 적용하거나 디렉토리에만 적용하거나 볼륨 내의 파일과 디렉토리에 모두 적용할 수 있습니다.

- 파일 및 디렉터리 보안

스토리지 객체 내의 모든 디렉토리 및 파일에 적용됩니다. 기본 설정입니다.

- 파일 보안

스토리지 객체 내의 모든 파일에 적용됩니다. 이 보안을 적용해도 디렉토리에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

- 디렉터리 보안

스토리지 객체 내의 모든 디렉토리에 적용됩니다. 이 보안을 적용해도 파일에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

추가 액세스 권한은 제공하지 않습니다.

- NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다.

스토리지 객체 레벨에서 적용되고 유효 사용 권한을 결정하는 데 사용되는 메타데이터에 저장됩니다.

- 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 보안을 취소할 수 없습니다.

스토리지 관리자만 수정할 수 있습니다.

- NTFS 또는 혼합 보안 스타일을 사용하는 볼륨에 스토리지 수준 액세스 가드를 적용할 수 있습니다.

- 볼륨이 포함된 SVM에 CIFS 서버가 구성되어 있는 경우 UNIX 보안 스타일을 사용하는 볼륨에 Storage-Level Access Guard를 적용할 수 있습니다.

- 볼륨이 볼륨 집합 경로 아래에 마운트되고 해당 경로에 Storage-Level Access Guard가 있는 경우 그 아래에 마운트된 볼륨으로 전파되지 않습니다.

- Storage-Level Access Guard 보안 설명자는 SnapMirror 데이터 복제 및 SVM 복제를 통해 복제됩니다.

- 바이러스 스캐너용 특별한 디스펜션이 있습니다.

저장소 수준 액세스 가드가 개체에 대한 액세스를 거부하더라도 이러한 서버에서 파일과 디렉토리를 선별하기 위해 예외적인 액세스가 허용됩니다.

- 스토리지 레벨 액세스 가드로 인해 액세스가 거부되면 FPolicy 알림이 전송되지 않습니다.

파일 또는 디렉토리에 대한 액세스는 내보내기 또는 공유 권한, 볼륨에 설정된 Storage-Level Access Guard 권한, 파일 및/또는 디렉토리에 적용되는 기본 파일 권한의 합집합에 의해 결정됩니다. 모든 보안 수준을 평가하여 파일 또는 디렉토리에 있는 유효한 권한을 결정합니다. 보안 액세스 검사는 다음 순서로 수행됩니다.

1. SMB 공유 또는 NFS 익스포트 레벨 사용 권한
2. 스토리지 레벨 액세스 가드
3. NTFS 파일/폴더 ACL(액세스 제어 목록), NFSv4 ACL 또는 UNIX 모드 비트

### Storage-Level Access Guard 사용 사례

Storage-Level Access Guard는 클라이언트 측에서 볼 수 없는 스토리지 수준에서 추가 보안을 제공하므로 사용자 또는 관리자가 데스크톱에서 해당 보안을 취소할 수 없습니다. 스토리지 레벨에서 액세스를 제어하는 기능이 유용하다고 볼 수 있는 특정 사용 사례가 있습니다.

이 기능의 일반적인 사용 사례는 다음과 같습니다.

- 스토리지 수준에서 모든 사용자의 액세스를 감사 및 제어하여 지적 재산을 보호합니다
- 은행 및 거래 그룹을 비롯한 금융 서비스 기업을 위한 스토리지
- 정부 서비스 및 개별 부서용 개별 파일 스토리지
- 모든 학생 파일을 보호하는 대학

### Storage-Level Access Guard를 구성하는 워크플로우

스토리지 레벨 액세스 가드(slag)를 구성하는 워크플로에서는 NTFS 파일 권한 및 감사 정책을 구성하는 데 사용하는 것과 동일한 ONTAP CLI 명령을 사용합니다. 지정된 대상에서 파일 및 디렉토리 액세스를 구성하는 대신 지정된 SVM(스토리지 가상 머신) 볼륨의 슬래그를 구성합니다.



관련 정보

[Storage-Level Access Guard 구성](#)

## Storage-Level Access Guard를 구성합니다

볼륨 또는 qtree에 스토리지 레벨 액세스 가드를 구성하려면 여러 단계를 수행해야 합니다. Storage-Level Access Guard는 스토리지 레벨에서 설정된 액세스 보안 수준을 제공합니다. 모든 NAS 프로토콜에서 적용된 스토리지 객체에 대한 모든 액세스에 적용되는 보안을 제공합니다.

### 단계

1. 'vserver security file-directory NTFS create' 명령을 사용하여 보안 설명자를 생성합니다.

```
'vserver security file-directory NTFS create-vserver vs1-ntfs-sd sd1"vserver security file-directory NTFS show-vserver vs1'
```

```
Vserver: vs1
```

NTFS Security Descriptor Name	Owner Name
sd1	-

보안 설명자는 다음 네 가지 기본 ACE(DACL 액세스 제어 항목)를 사용하여 만들어집니다.

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
BUILTIN\Administrators	allow	full-control	this-folder, sub-folders, files
BUILTIN\Users	allow	full-control	this-folder, sub-folders, files
CREATOR OWNER	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

Storage-Level Access Guard를 구성할 때 기본 항목을 사용하지 않으려면 보안 설명자에 고유한 ACE를 만들고 추가하기 전에 해당 항목을 제거할 수 있습니다.

2. Storage-Level Access Guard 보안으로 구성하지 않으려는 보안 설명자에서 기본 DACL ACE 중 하나를 제거합니다.

- a. 'vserver security file-directory NTFS DACL remove' 명령을 사용하여 불필요한 DACL ACE를 제거합니다.

이 예제에서는 세 개의 기본 DACL ACE가 보안 설명자인 BUILTIN\Administrators, BUILTIN\Users 및 Creator Owner에서 제거됩니다.

```
'vserver security file-directory NTFS DACL remove-vserver vs1-ntfs-sd SD1-access-type allow-account builtin\users"vserver security file-directory NTFS DACL remove-vserver vs1-directory vs1-access-directs builtl-creator' vserver security file-directs -directs -ntfs -directs -ntfs -directs -directs -creator
```

- b. 'vserver security file-directory NTFS DACL show' 명령을 사용하여 스토리지 수준 액세스 가드 보안에 사용하지 않을 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

이 예제에서 명령의 출력은 NT AUTHORITY\SYSTEM DEFAULT DACL ACE 항목만 남겨 두고 세 개의 기본 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

```
'vserver security file-directory NTFS DACL show -vserver vs1'
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

3. 'vserver security file-directory NTFS DACL add' 명령을 사용하여 하나 이상의 DACL 항목을 보안 설명자에 추가합니다.

이 예제에서는 보안 설명자에 두 개의 DACL ACE가 추가됩니다.

```
'vserver security file-directory NTFS DACL add-vserver vs1-ntfs-sd SD1-access-type allow-account example\engineering-rights full-control-apply-to this-folder, sub-folders, files"vserver security file-directory ntfs DACL add-vserver vs1-ntfs-access-type allow-account" example\Domain Users"-read-folders 폴더에 대한 읽기 권한
```

4. 'vserver security file-directory NTFS SACL add' 명령을 사용하여 하나 이상의 SACL 항목을 보안 설명자에 추가합니다.

이 예제에서는 두 개의 SACL ACE가 보안 설명자에 추가됩니다.

```
'vserver security file-directory NTFS SACL add-vserver vs1-ntfs-sd SD1-access-type failure-account' example\Domain Users"-rights read-apply-to this-folder, sub-folders, files"vserver security file-directory NTFS SACL add-vserver vs1-ntfs-sd-access-type success-account example\engineering-folders full-control-folders
```

5. 'vserver security file-directory NTFS DACL show' 및 'vserver security file-directory NTFS SACL show' 명령을 각각 사용하여 DACL 및 SACL ACE가 올바르게 구성되었는지 확인합니다.

이 예제에서 다음 명령은 보안 설명자 "Sd1"의 DACL 항목에 대한 정보를 표시합니다.

```
'vserver security file-directory NTFS DACL show -vserver vs1-NTFS-SD SD1'
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	allow	read	this-folder, sub-folders, files
EXAMPLE\engineering	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

이 예제에서 다음 명령은 보안 설명자 "sd1"에 대한 SACL 항목에 대한 정보를 표시합니다.

'vserver security file-directory NTFS SACL show -vserver vs1-NTFS-SD SD1'

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	failure	read	this-folder, sub-folders, files
EXAMPLE\engineering	success	full-control	this-folder, sub-folders, files

6. 'vserver security file-directory policy create' 명령을 사용하여 보안 정책을 생성합니다.

다음 예제에서는 ""정책1""이라는 정책을 만듭니다.

'vserver security file-directory policy create-vserver vs1-policy-name policy1'

7. 'vserver security file-directory policy show' 명령을 사용하여 정책이 올바르게 구성되었는지 확인합니다.

'vserver security file-directory policy show'를 선택합니다

Vserver	Policy Name
-----	-----
vs1	policy1

8. 을 사용하여 연결된 보안 설명자가 있는 작업을 보안 정책에 추가합니다 `vserver security file-directory policy task add` 명령과 함께 `-access-control` 매개 변수를 로 설정합니다 `slag`.

정책에 둘 이상의 Storage-Level Access Guard 작업이 포함될 수 있지만 파일 디렉터리 및 Storage-Level Access Guard 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉터리 작업이 포함되어야 합니다.

이 예제에서는 보안 설명자 'Sd1'에 할당된 "정책1"이라는 정책에 작업이 추가됩니다. 액세스 제어 유형이 '슬래그'로 설정된 '/datavol1' 경로에 할당됩니다.

'vserver security file-directory policy task add-vserver vs1-policy-name policy1-path/datavol1-access-control slag-security-type ntfs-ntfs-mode propagate-ntfs-sd SD1'

9. 'vserver security file-directory policy task show' 명령을 사용하여 작업이 올바르게 구성되었는지 확인합니다.

'vserver security file-directory policy task show -vserver vs1-policy-name policy1'

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	Descriptor
Name					
-----	-----	-----	-----	-----	-----
1	/datavol1	slag	ntfs	propagate	sd1

10. 'vserver security file-directory apply' 명령을 사용하여 Storage-Level Access Guard 보안 정책을 적용합니다.

'vserver security file-directory apply-vserver vs1-policy-name policy1'

보안 정책을 적용할 작업이 예약됩니다.

11. 'vserver security file-directory show' 명령을 사용하여 적용된 Storage-Level Access Guard 보안 설정이 올바른지 확인합니다.

이 예제에서 명령의 출력은 스토리지 레벨 액세스 가드 보안이 NTFS 볼륨 '/datavol1'에 적용되었음을 보여 줍니다. 모든 사용자에게 모든 권한을 허용하는 기본 DACL이 그대로 유지되더라도 Storage-Level Access Guard 보안은 Storage-Level Access Guard 설정에 정의된 그룹에 대한 액세스를 제한(및 감사)합니다.

'vserver security file-directory show -vserver vs1-path/datavol1'

```

        Vserver: vs1
        File Path: /datavol1
File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0x8004
              Owner:BUILTIN\Administrators
              Group:BUILTIN\Administrators
              DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

## 관련 정보

[CLI를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다](#)

[Storage-Level Access Guard를 구성하는 워크플로우](#)

[Storage-Level Access Guard에 대한 정보 표시](#)

[Storage-Level Access Guard 제거](#)



볼륨 또는 qtree 또는 둘 다에서 슬래그를 구성할 수 있습니다. 슬래그 매트릭스는 표에 나열된 다양한 시나리오에서 적용 가능한 슬래그 구성인 볼륨 또는 qtree를 정의합니다.

	<b>AFS</b> 에서 볼륨 슬래그	스냅샷 복사본의 볼륨 슬래그	<b>AFS</b> 에서 <b>qtree</b> 슬래그	스냅샷 복사본에서 <b>qtree</b> 슬래그 발생
AFS(Access File System)에서 볼륨 액세스	예	아니요	해당 없음	해당 없음
스냅샷 복사본의 볼륨 액세스	예	아니요	해당 없음	해당 없음
AFS에서 qtree 액세스(qtree에 슬래그가 있는 경우)	아니요	아니요	예	아니요
AFS에서 qtree 액세스(qtree에 슬래그가 없는 경우)	예	아니요	아니요	아니요
스냅샷 복사본에서 qtree 액세스(qtree AFS에 슬래그가 있는 경우)	아니요	아니요	예	아니요
스냅샷 복사본에서 qtree 액세스(qtree AFS에 슬래그가 없는 경우)	예	아니요	아니요	아니요

**Storage-Level Access Guard**에 대한 정보를 표시합니다

Storage-Level Access Guard는 볼륨 또는 qtree에 적용되는 세 번째 보안 계층입니다. Windows 속성 창을 사용하면 저장소 수준 액세스 가드 설정을 볼 수 없습니다. ONTAP CLI를 사용하여 스토리지 레벨 액세스 가드 보안에 대한 정보를 확인해야 합니다. 이 정보는 구성을 확인하거나 파일 액세스 문제를 해결하는 데 사용할 수 있습니다.

이 작업에 대해

SVM(Storage Virtual Machine)의 이름과 스토리지 레벨 액세스 가드 보안 정보를 표시할 볼륨 또는 qtree의 경로를 입력해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

단계

1. Storage-Level Access Guard 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver_vserver_name_-path_path_'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver_vserver_name_-path_path_-expand-mask true'

예

다음 예에서는 SVM VS1 에서 경로 '/datavol1'을 사용하여 NTFS 보안 스타일 볼륨에 대한 Storage-Level Access Guard 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에서 혼합 보안 형식 볼륨에 대한 Storage-Level Access Guard 정보를 표시합니다. 이 볼륨의 최상위 수준에는 UNIX의 효과적인 보안이 있습니다. 이 볼륨에는 Storage-Level Access Guard 보안이 있습니다.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

**Storage-Level Access Guard**를 제거합니다

저장소 수준에서 액세스 보안을 더 이상 설정하지 않으려면 볼륨 또는 qtree에서 저장소 수준 액세스 가드를 제거할 수 있습니다. Storage-Level Access Guard를 제거해도 일반 NTFS 파일 및 디렉터리 보안은 수정하거나 제거되지 않습니다.

단계

1. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에 Storage-Level Access Guard가 구성되어 있는지 확인합니다.

```
'vserver security file-directory show -vserver vs1-path/datavol2'
```

```

        Vserver: vs1
        File Path: /datavol2
    File Inode Number: 99
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0xbf14
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            SACL - ACEs
                AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
            DACL - ACEs
                ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

    Storage-Level Access Guard security
    DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Admins-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Admins-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. 'vserver security file-directory remove-slag' 명령을 사용하여 Storage-Level Access Guard를 제거합니다.

```
'vserver security file-directory remove-slag-vserver vs1-path/datavol2'
```

3. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에서 Storage-Level Access Guard가 제거되었는지 확인합니다.

```
'vserver security file-directory show -vserver vs1-path/datavol2'
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

```

## SMB를 사용하여 파일 액세스를 관리합니다

로컬 사용자 및 그룹을 인증 및 인증에 사용합니다

**ONTAP**에서 로컬 사용자 및 그룹을 사용하는 방법

로컬 사용자 및 그룹 개념

사용자 환경에서 로컬 사용자 및 그룹을 구성하고 사용할지 여부를 결정하기 전에 로컬 사용자 및 그룹의 정의 및 이에 대한 몇 가지 기본 정보를 알아야 합니다.

- \* 로컬 사용자 \*

생성된 SVM(스토리지 가상 머신)만 볼 수 있는 고유한 SID(보안 식별자)를 가진 사용자 계정 로컬 사용자 계정에는 사용자 이름 및 SID를 비롯한 일련의 속성이 있습니다. 로컬 사용자 계정은 NTLM 인증을 사용하여 CIFS 서버에서 로컬로 인증됩니다.

사용자 계정에는 여러 가지 용도가 있습니다.

- 사용자에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
- SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.

- \* 로컬 그룹 \*

고유한 SID가 있는 그룹은 해당 SID가 생성된 SVM에서만 볼 수 있습니다. 그룹에는 구성원 집합이 포함됩니다. 구성원은 로컬 사용자, 도메인 사용자, 도메인 그룹 및 도메인 컴퓨터 계정일 수 있습니다. 그룹을 생성, 수정 또는 삭제할 수 있습니다.

그룹은 여러 가지 용도로 사용됩니다.

- 해당 구성원에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
- SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.

- \* 로컬 도메인 \*

SVM에서 범위가 지정된 로컬 영역 로컬 도메인의 이름은 CIFS 서버 이름입니다. 로컬 사용자 및 그룹은 로컬 도메인 내에 포함됩니다.

- \* SID(보안 식별자) \*

SID는 Windows 스타일의 보안 주체를 식별하는 가변 길이 숫자 값입니다. 예를 들어 일반적인 SID는 S-1-5-21-3139654847-1303905135-2517279418-123456의 형태를 사용합니다.

- \* NTLM 인증 \*

CIFS 서버에서 사용자를 인증하는 데 사용되는 Microsoft Windows 보안 방법입니다.

- \* 클러스터 복제 데이터베이스(RDB) \*

클러스터의 각 노드에 인스턴스가 있는 복제된 데이터베이스입니다. 로컬 사용자 및 그룹 객체가 RDB에 저장됩니다.

로컬 사용자 및 로컬 그룹을 만드는 이유

SVM(스토리지 가상 시스템)에서 로컬 사용자 및 로컬 그룹을 생성하는 데는 여러 가지 이유가 있습니다. 예를 들어 DC(도메인 컨트롤러)를 사용할 수 없거나, 로컬 그룹을 사용하여 권한을 할당하거나, SMB 서버가 작업 그룹에 있는 경우 로컬 사용자 계정을 사용하여 SMB 서버에 액세스할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 사용자 계정을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 사용자를 사용할 수 없습니다.

로컬 사용자는 작업 그룹 구성에 필요합니다.

- 도메인 컨트롤러를 사용할 수 없는 경우 SMB 서버를 인증하고 로그인할 수 있어야 합니다.

로컬 사용자는 도메인 컨트롤러가 다운되었을 때 NTLM 인증을 사용하여 SMB 서버를 인증할 수 있으며, 네트워크 문제로 인해 SMB 서버가 도메인 컨트롤러에 접속할 수 없게 되는 경우

- 로컬 사용자에게 사용자 권한 관리 권한을 할당하려고 합니다.

*User Rights Management* 는 SMB 서버 관리자가 SVM에 대한 사용자 및 그룹의 권한을 제어할 수 있는 기능입니다. 사용자 계정에 권한을 할당하거나 해당 권한이 있는 로컬 그룹의 구성원으로 만들어 사용자에게 권한을 할당할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 그룹을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 그룹을 사용할 수 없습니다.

로컬 그룹은 작업 그룹 구성에 필요하지 않지만 로컬 작업 그룹 사용자에게 대한 액세스 권한을 관리하는 데 유용할 수 있습니다.

- 공유 및 파일 액세스 제어를 위해 로컬 그룹을 사용하여 파일 및 폴더 리소스에 대한 액세스를 제어하려는 경우
- Customized\_User Rights Management\_Privileges를 사용하여 로컬 그룹을 생성하려고 합니다.

일부 기본 제공 사용자 그룹에는 사전 정의된 권한이 있습니다. 사용자 지정된 권한 집합을 할당하려면 로컬 그룹을 생성하고 해당 그룹에 필요한 권한을 할당할 수 있습니다. 그런 다음 로컬 사용자, 도메인 사용자 및 도메인 그룹을 로컬 그룹에 추가할 수 있습니다.

## 관련 정보

### 로컬 사용자 인증의 작동 방식

### 지원되는 권한 목록입니다

#### 로컬 사용자 인증의 작동 방식

로컬 사용자가 CIFS 서버의 데이터를 액세스하려면 먼저 인증된 세션을 생성해야 합니다.

SMB는 세션 기반이므로 세션이 처음 설정될 때 사용자 ID를 한 번만 결정할 수 있습니다. CIFS 서버는 로컬 사용자를 인증할 때 NTLM 기반 인증을 사용합니다. NTLMv1과 NTLMv2가 모두 지원됩니다.

ONTAP은 세 가지 사용 사례에서 로컬 인증을 사용합니다. 각 활용 사례는 사용자 이름의 도메인 부분(domain\user 형식)이 CIFS 서버의 로컬 도메인 이름(CIFS 서버 이름)과 일치하는지 여부에 따라 달라집니다.

- 도메인 부분이 일치합니다

데이터에 대한 액세스를 요청할 때 로컬 사용자 자격 증명을 제공하는 사용자는 CIFS 서버에서 로컬로 인증됩니다.

- 도메인 부분이 일치하지 않습니다

ONTAP은 CIFS 서버가 속한 도메인의 도메인 컨트롤러에서 NTLM 인증을 사용하려고 합니다. 인증에 성공하면 로그인이 완료된 것입니다. 성공하지 못하면 다음 단계는 인증이 성공하지 못한 이유에 따라 달라집니다.

예를 들어 사용자가 Active Directory에 있지만 암호가 잘못되었거나 만료된 경우 ONTAP은 CIFS 서버에서 해당 로컬 사용자 계정을 사용하지 않습니다. 대신 인증에 실패합니다. ONTAP가 CIFS 서버에 있는 경우 NetBIOS 도메인 이름이 일치하지 않아도 인증을 위해 해당 로컬 계정을 사용하는 경우도 있습니다. 예를 들어 일치하는 도메인 계정이 있지만 비활성화된 경우 ONTAP은 CIFS 서버에서 해당 로컬 계정을 사용하여 인증합니다.

- 도메인 부분이 지정되지 않았습니다

ONTAP은 먼저 로컬 사용자로 인증을 시도합니다. 로컬 사용자로 인증에 실패하면 ONTAP은 CIFS 서버가 속한 도메인의 도메인 컨트롤러를 사용하여 사용자를 인증합니다.

로컬 또는 도메인 사용자 인증이 성공적으로 완료되면 ONTAP은 로컬 그룹 구성원 자격 및 권한을 고려하여 전체 사용자 액세스 토큰을 생성합니다.



로컬 사용자의 NTLM 인증에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

관련 정보

## 로컬 사용자 인증 활성화 또는 비활성화

사용자 액세스 토큰을 구성하는 방법입니다

사용자가 공유를 매핑하면 인증된 SMB 세션이 설정되고 사용자, 사용자의 그룹 구성원 자격 및 누적 권한, 매핑된 UNIX 사용자에 대한 정보가 포함된 사용자 액세스 토큰이 생성됩니다.

이 기능을 사용하지 않는 한 로컬 사용자 및 그룹 정보도 사용자 액세스 토큰에 추가됩니다. 액세스 토큰이 구성되는 방식은 로컬 사용자에 대한 로그인인지 Active Directory 도메인 사용자에 대한 로그인인지에 따라 달라집니다.

- 로컬 사용자 로그인입니다

로컬 사용자는 다른 로컬 그룹의 구성원이 될 수 있지만 로컬 그룹은 다른 로컬 그룹의 구성원이 될 수 없습니다. 로컬 사용자 액세스 토큰은 특정 로컬 사용자가 구성원인 그룹에 할당된 모든 권한의 합집합으로 구성됩니다.

- 도메인 사용자 로그인

도메인 사용자가 로그인하면 ONTAP는 사용자가 구성원인 모든 도메인 그룹의 사용자 SID 및 SID가 포함된 사용자 액세스 토큰을 얻습니다. ONTAP는 도메인 사용자 액세스 토큰의 조합과 사용자의 도메인 그룹(있는 경우)의 로컬 멤버십에서 제공하는 액세스 토큰, 도메인 사용자 또는 해당 도메인 그룹 구성원에 할당된 모든 직접 권한을 사용합니다.

로컬 및 도메인 사용자 로그인의 경우 사용자 액세스 토큰에 대해 기본 그룹 제거도 설정됩니다. 기본 RID는 Domain Users(RID 513)입니다. 기본값을 변경할 수 없습니다.

Windows-to-UNIX 및 UNIX-to-Windows 이름 매핑 프로세스는 로컬 및 도메인 계정에 대해 동일한 규칙을 따릅니다.



UNIX 사용자에서 로컬 계정으로 자동 매핑은 암시적으로 수행되지 않습니다. 이 작업이 필요한 경우 기존 이름 매핑 명령을 사용하여 명시적 매핑 규칙을 지정해야 합니다.

로컬 그룹이 포함된 SVM에서 SnapMirror 사용 지침

로컬 그룹이 포함된 SVM이 소유한 볼륨에 SnapMirror를 구성할 때는 지침을 숙지해야 합니다.

SnapMirror에서 다른 SVM으로 복제된 파일, 디렉토리 또는 공유에 적용된 ACE의 로컬 그룹은 사용할 수 없습니다. SnapMirror 기능을 사용하여 다른 SVM의 볼륨에 DR 미러를 생성하고 볼륨에 로컬 그룹에 ACE가 있는 경우 ACE는 미러에서 유효하지 않습니다. 데이터를 다른 SVM으로 복제하면 데이터가 다른 로컬 도메인에 효과적으로 교차합니다. 로컬 사용자 및 그룹에 부여되는 사용 권한은 원래 생성된 SVM의 범위 내에서만 유효합니다.

CIFS 서버를 삭제할 때 로컬 사용자 및 그룹이 어떻게 됩니까

CIFS 서버가 생성될 때 로컬 사용자 및 그룹의 기본 세트가 생성되고 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)과 연결됩니다. SVM 관리자는 언제든지 로컬 사용자 및 그룹을 생성할 수 있습니다. CIFS 서버를 삭제할 때 로컬 사용자 및 그룹에 어떤 일이 발생하는지 알고 있어야 합니다.

로컬 사용자 및 그룹은 SVM에 연결되어 있으므로 보안 고려 사항으로 인해 CIFS 서버를 삭제할 때 삭제되지 않습니다.

CIFS 서버가 삭제되어도 로컬 사용자 및 그룹은 삭제되지 않지만 숨겨집니다. SVM에서 CIFS 서버를 다시 생성할 때까지 로컬 사용자 및 그룹을 보거나 관리할 수 없습니다.



CIFS 서버 관리 상태는 로컬 사용자 또는 그룹의 표시에는 영향을 주지 않습니다.

로컬 사용자 및 그룹과 함께 **Microsoft Management Console**을 사용하는 방법

Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 정보를 볼 수 있습니다. 이 ONTAP 릴리스에서는 Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 다른 관리 작업을 수행할 수 없습니다.

되돌리기 지침

로컬 사용자 및 그룹을 지원하지 않는 ONTAP 릴리즈로 클러스터를 되돌리려는 경우 로컬 사용자 및 그룹을 사용하여 파일 액세스 또는 사용자 권한을 관리하려면 특정 고려 사항을 알고 있어야 합니다.

- 보안상의 이유로 ONTAP가 로컬 사용자 및 그룹 기능을 지원하지 않는 버전으로 되돌려지면 구성된 로컬 사용자, 그룹 및 권한에 대한 정보가 삭제되지 않습니다.
- ONTAP의 이전 주요 버전으로 되돌릴 때 ONTAP는 인증 및 자격 증명 생성 중에 로컬 사용자 및 그룹을 사용하지 않습니다.
- 로컬 사용자 및 그룹은 파일 및 폴더 ACL에서 제거되지 않습니다.
- 로컬 사용자 또는 그룹에 부여된 권한으로 인해 부여되는 액세스에 의존하는 파일 액세스 요청이 거부됩니다.

액세스를 허용하려면 로컬 사용자 및 그룹 개체 대신 도메인 개체를 기반으로 액세스를 허용하도록 파일 권한을 다시 구성해야 합니다.

어떤 로컬 권한이 있는지 확인합니다

지원되는 권한 목록입니다

ONTAP에는 지원되는 권한이 미리 정의되어 있습니다. 미리 정의된 특정 로컬 그룹에는 이러한 권한 중 일부가 기본적으로 추가됩니다. 또한 미리 정의된 그룹에서 권한을 추가하거나 제거하거나 새 로컬 사용자 또는 그룹을 만들고 만든 그룹 또는 기존 도메인 사용자 및 그룹에 권한을 추가할 수도 있습니다.

다음 표에는 SVM(스토리지 가상 시스템)에서 지원되는 권한이 나열되어 있으며 할당된 권한이 있는 BUILTIN 그룹 목록이 제공됩니다.

권한 이름입니다	기본 보안 설정입니다	설명
'세TcbPrivilege'입니다	없음	운영 체제의 일부로 작동합니다
'BackupPrivilege'입니다	'BUILTIN\Administrators', 'BUILTIN\Backup Operators'	파일 및 디렉토리를 백업하고 모든 ACL을 재정의합니다

권한 이름입니다	기본 보안 설정입니다	설명
스저장창고특권	'BUILTIN\Administrators', 'BUILTIN\Backup Operators'	파일 및 디렉토리를 복원하고 모든 ACL을 재정의하면 유효한 사용자 또는 그룹 SID가 파일 소유자로 설정됩니다
'새테이크오너선프리빌리지'	'BUILTIN\Administrators'	파일 또는 기타 개체의 소유권을 가져옵니다
'보안 권한'	'BUILTIN\Administrators'	감사 관리  여기에는 보안 로그 보기, 덤프 및 지우기가 포함됩니다.
'스변경NotifyPrivilege'입니다	'BUILTIN\Administrators', 'BUILTIN\Backup Operators', 'BUILTIN\Power Users', 'BUILTIN\Users', 'Everyone'	횡단 검사를 무시합니다  이 권한이 있는 사용자는 폴더, 교집합 또는 교차로를 횡단(x) 권한이 필요하지 않습니다.

#### 관련 정보

- [로컬 권한을 할당합니다](#)
- [통과 확인 우회 구성](#)

#### 권한을 할당합니다

로컬 사용자 또는 도메인 사용자에게 직접 권한을 할당할 수 있습니다. 또는 할당된 권한이 해당 사용자에게 부여할 기능과 일치하는 로컬 그룹에 사용자를 할당할 수 있습니다.

- 생성한 그룹에 권한 집합을 할당할 수 있습니다.

그런 다음 해당 사용자에게 부여할 권한이 있는 사용자를 그룹에 추가합니다.

- 기본 권한이 해당 사용자에게 부여할 권한과 일치하는 미리 정의된 그룹에 로컬 사용자 및 도메인 사용자를 할당할 수도 있습니다.

#### 관련 정보

- [로컬 또는 도메인 사용자 또는 그룹에 권한 추가](#)
- [로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거합니다](#)
- [로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정합니다](#)
- [통과 확인 우회 구성](#)

#### BUILTIN 그룹 및 로컬 관리자 계정 사용에 대한 지침

BUILTIN 그룹 및 로컬 관리자 계정을 사용할 때 유의해야 할 몇 가지 지침이 있습니다. 예를 들어 로컬 관리자 계정의 이름을 바꿀 수는 있지만 이 계정은 삭제할 수 없습니다.

- Administrator 계정의 이름을 바꿀 수는 있지만 삭제할 수는 없습니다.
- 관리자 계정은 BUILTIN\Administrators 그룹에서 제거할 수 없습니다.
- BUILTIN 그룹은 이름을 바꿀 수 있지만 삭제할 수 없습니다.

BUILTIN 그룹의 이름을 바꾼 후 잘 알려진 이름으로 다른 로컬 개체를 만들 수 있지만 개체에 새 RID가 할당됩니다.

- 로컬 게스트 계정이 없습니다.

관련 정보

[사전 정의된 BUILTIN 그룹 및 기본 권한](#)

로컬 사용자 암호 요구 사항

기본적으로 로컬 사용자 암호는 복잡성 요구 사항을 충족해야 합니다. 암호 복잡성 요구 사항은 Microsoft Windows\_Local 보안 정책 \_에 정의된 요구 사항과 비슷합니다.

암호는 다음 기준을 충족해야 합니다.

- 6자 이상이어야 합니다
- 사용자 계정 이름을 포함해서는 안 됩니다
- 다음 4개 범주 중 3개 이상의 문자를 포함해야 합니다.
  - 영어 대문자(A ~ Z)
  - 영어 소문자(a ~ z)
  - 기본 10자리(0 ~ 9)
  - 특수 문자:

~! @#\$%^ & \* \_-+="\\()[]:;<>,. ? /

관련 정보

[로컬 SMB 사용자에게 대한 필수 암호 복잡성 활성화 또는 비활성화](#)

[CIFS 서버 보안 설정에 대한 정보를 표시합니다](#)

[로컬 사용자 계정 암호 변경](#)

사전 정의된 **BUILTIN** 그룹 및 기본 권한

ONTAP에서 제공하는 미리 정의된 BUILTIN 그룹 집합에 로컬 사용자 또는 도메인 사용자의 구성원을 할당할 수 있습니다. 사전 정의된 그룹에는 사전 정의된 권한이 할당됩니다.

다음 표에는 미리 정의된 그룹이 설명되어 있습니다.

미리 정의된 <b>BUILTIN</b> 그룹	기본 권한
<p>"BUILTIN\Administrators" RID 544</p> <p>처음 만들어지면 500여 개 계정을 없앤다고 하면 자동으로 이 그룹의 회원이 됩니다. SVM(Storage Virtual Machine)이 도메인에 가입되면 domain\Domain Admins 그룹이 그룹에 추가됩니다. SVM이 도메인을 벗어나면 domain\Domain Admins 그룹이 그룹에서 제거됩니다.</p>	<ul style="list-style-type: none"> <li>• 'BackupPrivilege'입니다</li> <li>• 스토리지창고특권</li> <li>• '보안 권한'</li> <li>• '새테이크오너선프리빌리지'</li> <li>• '스변경NotifyPrivilege'입니다</li> </ul>
<p>"BUILTIN\Power Users" RID 547</p> <p>이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 다음과 같은 특성을 갖습니다.</p> <ul style="list-style-type: none"> <li>• 로컬 사용자 및 그룹을 생성하고 관리할 수 있습니다.</li> <li>• 자체 또는 다른 개체를 'BUILTIN\Administrators' 그룹에 추가할 수 없습니다.</li> </ul>	<p>'스변경NotifyPrivilege'입니다</p>
<p>"BUILTIN\Backup Operators" RID 551</p> <p>이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 백업 의도로 열린 파일 또는 폴더에 대한 읽기 및 쓰기 권한을 재정의할 수 있습니다.</p>	<ul style="list-style-type: none"> <li>• 'BackupPrivilege'입니다</li> <li>• 스토리지창고특권</li> <li>• '스변경NotifyPrivilege'입니다</li> </ul>
<p>"BUILTIN\Users" RID 545</p> <p>처음 만들어도 이 그룹에는 인증된 사용자 특별 그룹 외에 구성원이 없습니다. SVM이 도메인에 가입되면 이 그룹에 domain\Domain Users" 그룹이 추가됩니다. SVM이 도메인을 벗어나면 이 그룹에서 "도메인 사용자" 그룹이 제거됩니다.</p>	<p>'스변경NotifyPrivilege'입니다</p>
<p>모든 사람의 ID S-1-0입니다</p> <p>이 그룹에는 게스트(익명 사용자 제외)를 포함한 모든 사용자가 포함됩니다. 이 그룹은 묵시적 멤버십을 가진 암시적 그룹입니다.</p>	<p>'스변경NotifyPrivilege'입니다</p>

#### 관련 정보

[BUILTIN 그룹 및 로컬 관리자 계정 사용에 대한 지침](#)

[지원되는 권한 목록입니다](#)

[통과 확인 우회 구성](#)

로컬 사용자 및 그룹 기능을 설정하거나 해제합니다

로컬 사용자 및 그룹 기능 개요를 설정하거나 해제합니다

NTFS 보안 스타일 데이터의 액세스 제어에 로컬 사용자 및 그룹을 사용하려면 먼저 로컬 사용자 및 그룹 기능을 활성화해야 합니다. 또한 SMB 인증에 로컬 사용자를 사용하려면 로컬 사용자 인증 기능을 활성화해야 합니다.

로컬 사용자 및 그룹 기능 및 로컬 사용자 인증은 기본적으로 사용됩니다. 이 옵션이 설정되어 있지 않으면 로컬 사용자 및 그룹을 구성하고 사용할 수 있도록 설정하기 전에 설정해야 합니다. 언제든지 로컬 사용자 및 그룹 기능을 사용하지 않도록 설정할 수 있습니다.

로컬 사용자 및 그룹 기능을 명시적으로 해제하는 것 외에도, 클러스터의 노드가 해당 기능을 지원하지 않는 ONTAP 릴리즈로 되돌려지는 경우 ONTAP는 로컬 사용자 및 그룹 기능을 비활성화합니다. 클러스터의 모든 노드에서 지원하는 ONTAP 버전이 실행될 때까지 로컬 사용자 및 그룹 기능이 활성화되지 않습니다.

관련 정보

[로컬 사용자 계정을 수정합니다](#)

[로컬 그룹을 수정합니다](#)

[로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다](#)

로컬 사용자 및 그룹을 설정하거나 해제합니다

SVM(스토리지 가상 머신)에서 SMB 액세스를 위해 로컬 사용자 및 그룹을 설정하거나 해제할 수 있습니다. 로컬 사용자 및 그룹 기능은 기본적으로 활성화되어 있습니다.

이 작업에 대해

SMB 공유 및 NTFS 파일 권한을 구성할 때 로컬 사용자 및 그룹을 사용할 수 있으며 SMB 연결을 생성할 때 로컬 사용자를 인증에 사용할 수도 있습니다. 로컬 사용자를 인증에 사용하려면 로컬 사용자 및 그룹 인증 옵션도 활성화해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

로컬 사용자 및 그룹을 사용하려는 경우...	명령 입력...
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-local-users-and-groups -enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-local-users-and-groups -enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 SVM VS1 에서 로컬 사용자 및 그룹 기능을 사용하도록 설정합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options modify -vsserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

## 관련 정보

[로컬 사용자 인증을 사용하거나 사용하지 않도록 설정합니다](#)

[로컬 사용자 계정을 설정하거나 해제합니다](#)

로컬 사용자 인증을 사용하거나 사용하지 않도록 설정합니다

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 로컬 사용자 인증을 설정하거나 해제할 수 있습니다. 기본값은 로컬 사용자 인증을 허용하는 것입니다. 이는 SVM이 도메인 컨트롤러에 연결할 수 없거나 도메인 레벨 액세스 제어를 사용하지 않도록 선택하는 경우에 유용합니다.

## 시작하기 전에

CIFS 서버에서 로컬 사용자 및 그룹 기능을 설정해야 합니다.

## 이 작업에 대해

언제든지 로컬 사용자 인증을 활성화 또는 비활성화할 수 있습니다. SMB 연결을 생성할 때 인증에 로컬 사용자를 사용하려면 CIFS 서버의 로컬 사용자 및 그룹 옵션도 설정해야 합니다.

## 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

로컬 인증을 사용하려는 경우...	명령 입력...
활성화됨	'vsserver cifs options modify -vsserver_vsserver_name_-is-local-auth-enabled true'
사용 안 함	'vsserver cifs options modify -vsserver_vsserver_name_-is-local-auth-enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

## 예

다음 예에서는 SVM VS1 에서 로컬 사용자 인증을 사용합니다.

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options modify -vsserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

## 관련 정보

### 로컬 사용자 인증의 작동 방식

### 로컬 사용자 및 그룹 활성화 또는 비활성화

### 로컬 사용자 계정을 관리합니다

### 로컬 사용자 계정을 수정합니다

기존 사용자의 전체 이름 또는 설명을 변경하고 사용자 계정을 활성화하거나 비활성화하려면 로컬 사용자 계정을 수정할 수 있습니다. 사용자 이름이 손상되었거나 관리를 위해 이름 변경이 필요한 경우 로컬 사용자 계정의 이름을 바꿀 수도 있습니다.

원하는 작업	명령 입력...
로컬 사용자의 전체 이름을 수정합니다	'vsserver cifs users-and-groups local-user modify -vsserver_vserver_name _user-name_user_name_-full-name text' 전체 이름에 공백이 포함되어 있으면 큰따옴표로 묶어야 합니다.
로컬 사용자의 설명을 수정합니다	'vsserver cifs users-and-groups local-user modify -vsserver_vserver_name _user-name_user_name_-description text' 설명에 공백이 포함된 경우 큰따옴표로 묶어야 합니다.
로컬 사용자 계정을 활성화하거나 비활성화합니다	'vsserver cifs users-and-groups local-user modify -vsserver_vserver_name _user-name_user_name_-is-account-disabled{true
false}'	로컬 사용자 계정의 이름을 바꿉니다

## 예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 로컬 사용자 "cifs\_server\sue"를 "cifs\_server\sue\_new"로 바꿉니다.1



```
cluster1::> vsserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vsserver vs1
```

로컬 사용자 계정을 설정하거나 해제합니다

사용자가 SMB 연결을 통해 SVM(스토리지 가상 머신)에 포함된 데이터에 액세스할 수 있도록 하려면 로컬 사용자 계정을 활성화합니다. 사용자가 SMB를 통해 SVM 데이터에 액세스하지 못하도록 하려면 로컬 사용자 계정을 사용하지 않도록 설정할 수도 있습니다.

이 작업에 대해

사용자 계정을 수정하여 로컬 사용자를 활성화할 수 있습니다.

단계

1. 적절한 작업을 수행합니다.

원하는 작업	명령 입력...
사용자 계정을 활성화합니다	'vsserver cifs users-and-groups local-user modify -vsserver_vserver_name_-user-name_user_name_-is-account-disabled false'
사용자 계정을 비활성화합니다	'vsserver cifs users-and-groups local-user modify -vsserver_vserver_name_-user-name_user_name_-is-account-disabled true'

로컬 사용자 계정 암호를 변경합니다

로컬 사용자의 계정 암호를 변경할 수 있습니다. 이 방법은 사용자의 암호가 손상되었거나 사용자가 암호를 잊어버린 경우에 유용합니다.

단계

1. 'vsserver cifs users-and-groups local-user set-password-vsserver\_vserver\_name\_-user-name\_user\_name\_' 작업을 수행하여 암호를 변경하십시오

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 과 연관된 로컬 사용자 "cifs\_server\sue"의 암호를 설정합니다.

```
cluster1::> vsserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vsserver vs1
```

```
Enter the new password:
Confirm the new password:
```

관련 정보

## 로컬 SMB 사용자에게 대한 필수 암호 복잡성 활성화 또는 비활성화

### CIFS 서버 보안 설정에 대한 정보를 표시합니다

로컬 사용자에게 대한 정보를 표시합니다

모든 로컬 사용자의 목록을 요약 양식에 표시할 수 있습니다. 특정 사용자에게 대해 구성된 계정 설정을 확인하려면 해당 사용자에게 대한 자세한 계정 정보와 여러 사용자에게 대한 계정 정보를 표시할 수 있습니다. 이 정보를 통해 사용자 설정을 수정해야 하는지 여부를 확인하고 인증 또는 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

사용자 암호에 대한 정보는 표시되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
SVM(스토리지 가상 시스템)의 모든 사용자에게 대한 정보 표시	'vserver cifs users-and-groups local-user show -vserver_vserver_name_'
사용자에게 대한 자세한 계정 정보를 표시합니다	'vserver cifs users-and-groups local-user show-instance-vserver_vserver_name_-user-name_user_name_'

명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

예

다음 예제는 SVM VS1의 모든 로컬 사용자에게 대한 정보를 표시합니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                Full Name                Description
-----
vs1      CIFS_SERVER\Administrator James Smith              Built-in administrator
account
vs1      CIFS_SERVER\sue          Sue    Jones
```

로컬 사용자의 그룹 구성원 자격에 대한 정보를 표시합니다

로컬 사용자가 속한 로컬 그룹에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 파일 및 폴더에 대한 사용자의 액세스 권한을 결정할 수 있습니다. 이 정보는 사용자가 파일 및 폴더에 대해 가질 액세스 권한을 결정하거나 파일 액세스 문제를 해결할 때 유용할 수 있습니다.

이 작업에 대해

명령을 사용자 지정하여 표시할 정보만 표시할 수 있습니다.

## 단계

### 1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
지정된 로컬 사용자의 로컬 사용자 구성원 정보를 표시합니다	'vserver cifs users-and-groups local-user show-membership-user_name_user_name_'
이 로컬 사용자가 구성원인 로컬 그룹의 로컬 사용자 구성원 정보를 표시합니다	'vserver cifs users-and-groups local-user show-membership_group_name_'
지정된 SVM(스토리지 가상 머신)과 연결된 로컬 사용자의 사용자 구성원 정보를 표시합니다.	'vserver cifs users-and-groups local-user show-membership-vserver_vserver_name_'
지정된 SVM의 모든 로컬 사용자에 대한 세부 정보를 표시합니다	'vserver cifs users-and-groups local-user show-membership-instance-vserver_vserver_name_'

## 예

다음 예에서는 SVM VS1 상의 모든 로컬 사용자에 대한 구성원 정보를 표시합니다. 사용자 "cifs\_server\Administrator"는 "BUILTIN\Administrators" 그룹의 구성원이고 "cifs\_server\sue"는 "cifs\_server\G1" 그룹의 구성원입니다.

```
cluster1::> vsriver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver      User Name                      Membership
-----
vs1          CIFS_SERVER\Administrator      BUILTIN\Administrators
            CIFS_SERVER\sue              CIFS_SERVER\g1
```

로컬 사용자 계정을 삭제합니다

CIFS 서버에 대한 로컬 SMB 인증이 더 이상 필요하지 않거나 SVM에 포함된 데이터에 대한 액세스 권한을 결정하기 위해 SVM(스토리지 가상 시스템)에서 로컬 사용자 계정을 삭제할 수 있습니다.

이 작업에 대해

로컬 사용자를 삭제할 때 다음 사항에 유의하십시오.

- 파일 시스템이 변경되지 않았습니다.
- 이 사용자를 참조하는 파일 및 디렉토리의 Windows 보안 설명자는 조정되지 않습니다.
- 로컬 사용자에 대한 모든 참조는 멤버 자격 및 권한 데이터베이스에서 제거됩니다.
- Administrator와 같이 잘 알려진 표준 사용자는 삭제할 수 없습니다.

## 단계

1. 삭제할 로컬 사용자 계정의 이름을 확인합니다. 'vserver cifs users-and-groups local-user show -vserver\_vserver\_name\_'
2. 로컬 사용자 'vserver cifs users-and-groups local-user delete -vserver\_vserver\_name\_-user-name\_username\_name\_'을 삭제합니다
3. 사용자 계정이 삭제되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver\_vserver\_name\_'

예

다음 예에서는 SVM VS1 관련 로컬 사용자 ""cifs\_server\sue""를 삭제합니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver   User Name                               Full Name           Description
-----
vs1       CIFS_SERVER\Administrator             James Smith         Built-in administrator
account
vs1       CIFS_SERVER\sue                      Sue    Jones

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver   User Name                               Full Name           Description
-----
vs1       CIFS_SERVER\Administrator             James Smith         Built-in administrator
account
```

로컬 그룹을 관리합니다

로컬 그룹을 수정합니다

기존 로컬 그룹에 대한 설명을 변경하거나 그룹의 이름을 변경하여 기존 로컬 그룹을 수정할 수 있습니다.

원하는 작업	명령 사용...
로컬 그룹 설명을 수정합니다	'vserver cifs users-and-groups local-group modify -vserver_vserver_name_-group-name_group_name_-description text' 설명에 공백이 포함되어 있으면 큰따옴표로 묶어야 합니다.
로컬 그룹의 이름을 바꿉니다	'vserver cifs users-and-groups local-group rename -vserver_vserver_name_-group-name_group_name_-new-group-name_new_group_name_'

예

다음 예에서는 로컬 그룹 "cifs\_server\engineering"의 이름을 "cifs\_server\engineering\_new"로 바꿉니다.

```
cluster1::> vservers cifs users-and-groups local-group rename -vservers vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

다음 예에서는 로컬 그룹 "cifs\_server\engineering"의 설명을 수정합니다.

```
cluster1::> vservers cifs users-and-groups local-group modify -vservers vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

로컬 그룹에 대한 정보를 표시합니다

클러스터 또는 지정된 SVM(스토리지 가상 머신)에 구성된 모든 로컬 그룹 목록을 표시할 수 있습니다. 이 정보는 SVM에 포함된 데이터에 대한 파일 액세스 문제 또는 SVM의 사용자 권한(권한) 문제를 해결할 때 유용할 수 있습니다.

단계

- 1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 원할 경우...	명령 입력...
클러스터의 모든 로컬 그룹입니다	'vservers cifs users-and-groups local-group show'를 참조하십시오
SVM의 모든 로컬 그룹	'vservers cifs users-and-groups local-group show -vservers vservers_name_'

이 명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

예

다음 예제는 SVM VS1의 모든 로컬 그룹에 대한 정보를 표시합니다.

```
cluster1::> vservers cifs users-and-groups local-group show -vservers vs1
Vserver  Group Name                                Description
-----  -
vs1      BUILTIN\Administrators                   Built-in Administrators group
vs1      BUILTIN\Backup Operators                  Backup Operators group
vs1      BUILTIN\Power Users                       Restricted administrative privileges
vs1      BUILTIN\Users                            All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

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 사용자에게 해당 그룹에 연결된 권한을 부여하려는 경우에 유용합니다.

이 작업에 대해

로컬 그룹에 구성원을 추가하기 위한 지침:

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

로컬 그룹에서 구성원을 제거하는 지침:

- special\_everyone\_group에서 구성원을 제거할 수 없습니다.
- 구성원을 제거할 그룹이 있어야 합니다.
- ONTAP는 그룹에서 제거하려는 구성원 이름을 해당 SID로 확인할 수 있어야 합니다.

단계

1. 그룹에서 구성원을 추가 또는 제거합니다.

원하는 작업	그런 다음 명령을 사용합니다...
그룹에 구성원을 추가합니다	'vserver cifs users-and-groups local-group add-member-vserver_name_-group-name_group_name_-member-names name[,...]'지정된 로컬 그룹에 추가할 심표로 구분된 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 목록을 지정할 수 있습니다.
그룹에서 구성원을 제거합니다	'vserver cifs users-and-groups local-group remove-memembers-vserver_name_-group-name_group_name_-member-names name[,...]'지정된 로컬 그룹에서 제거할 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 심표로 구분된 목록을 지정할 수 있습니다.

다음 예에서는 SVM VS1 상의 로컬 그룹 "sMB\_server\sue"와 도메인 그룹 "AD\_DOM\DOM\_ENG"를 로컬 그룹 "sMB\_server\engineering"에 추가합니다.

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

다음 예에서는 SVM VS1 로컬 그룹 "sMB\_server\sue"와 "sMB\_server\james"를 SVM VS1 로컬 그룹 "sMB\_server\engineering"에서 제거합니다.

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

## 관련 정보

### 로컬 그룹 구성원에 대한 정보 표시

로컬 그룹 구성원에 대한 정보를 표시합니다

클러스터 또는 지정된 SVM(스토리지 가상 머신)에 구성된 로컬 그룹의 모든 구성원 목록을 표시할 수 있습니다. 이 정보는 파일 액세스 문제 또는 사용자 권한(권한) 문제를 해결할 때 유용할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	명령 입력...
클러스터의 모든 로컬 그룹의 구성원입니다	'vserver cifs users-and-groups local-group show-ups'
SVM에 있는 모든 로컬 그룹의 구성원	'vserver cifs users-and-groups local-group show-ners-vserver_vserver_name_'

## 예

다음 예는 SVM VS1 로컬 그룹의 모든 구성원에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs users-and-groups local-group show-members
-vserver vs1
```

Vserver	Group Name	Members
vs1	BUILTIN\Administrators	CIFS_SERVER\Administrator AD_DOMAIN\Domain Admins AD_DOMAIN\dom_grp1
	BUILTIN\Users	AD_DOMAIN\Domain Users AD_DOMAIN\dom_usr1
	CIFS_SERVER\engineering	CIFS_SERVER\james

로컬 그룹을 삭제합니다

SVM(스토리지 가상 시스템)에서 로컬 그룹을 삭제하여 해당 SVM과 관련된 데이터에 대한 액세스 권한을 결정하거나 SVM 사용자 권한(권한)을 그룹 멤버에 할당할 필요가 없는 경우 해당 로컬 그룹을 삭제할 수 있습니다.

이 작업에 대해

로컬 그룹을 삭제할 때 다음 사항에 유의하십시오.

- 파일 시스템이 변경되지 않았습니다.
- 이 그룹을 참조하는 파일 및 디렉토리의 Windows 보안 설명자는 조정되지 않습니다.
- 그룹이 없으면 오류가 반환됩니다.
- special\_everyone\_group은 삭제할 수 없습니다.
- BUILTIN\Administrators\_\_BUILTIN\Users\_와 같은 기본 제공 그룹은 삭제할 수 없습니다.

단계

1. SVM에 로컬 그룹 목록을 표시하여 삭제할 로컬 그룹의 이름을 확인합니다. 'vsriver cifs users-and-groups local-group show -vserver vserver\_name'
2. 로컬 그룹 'vsriver cifs users-and-groups local-group delete -vserver\_vserver\_name\_-group-name\_group\_name\_'을 삭제합니다
3. 그룹이 삭제되었는지 확인합니다. 'vsriver cifs users-and-groups local-user show -vserver\_vserver\_name\_'

예

다음 예에서는 SVM VS1 관련 로컬 그룹 ""cifs\_server\sales""를 삭제합니다.



```

cluster1::> vsserver cifs users-and-groups local-group show -vsserver vs1
Vserver      Group Name          Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
vs1          BUILTIN\Power Users    Restricted administrative
privileges
vs1          BUILTIN\Users          All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales

cluster1::> vsserver cifs users-and-groups local-group delete -vsserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vsserver cifs users-and-groups local-group show -vsserver vs1
Vserver      Group Name          Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
vs1          BUILTIN\Power Users    Restricted administrative
privileges
vs1          BUILTIN\Users          All users
vs1          CIFS_SERVER\engineering

```

로컬 데이터베이스에서 도메인 사용자 및 그룹 이름을 업데이트합니다

CIFS 서버의 로컬 그룹에 도메인 사용자 및 그룹을 추가할 수 있습니다. 이러한 도메인 개체는 클러스터의 로컬 데이터베이스에 등록됩니다. 도메인 개체의 이름이 변경된 경우 로컬 데이터베이스를 수동으로 업데이트해야 합니다.

이 작업에 대해

도메인 이름을 업데이트할 SVM(스토리지 가상 시스템)의 이름을 지정해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 적절한 작업을 수행합니다.

도메인 사용자 및 그룹을 업데이트하려면 다음을 수행합니다.	이 명령 사용...
성공적으로 업데이트되었지만 업데이트에 실패한 도메인 사용자 및 그룹을 표시합니다	'vsserver cifs users-and-groups update-names-vsserver_vsserver_name_'
성공적으로 업데이트된 도메인 사용자 및 그룹을 표시합니다	'vsserver cifs users-and-groups update-names-vsserver_vsserver_name_-display-failed-only false'

도메인 사용자 및 그룹을 업데이트하려면 다음을 수행합니다.	이 명령 사용...
업데이트에 실패한 도메인 사용자 및 그룹만 표시합니다	'vserver cifs users-and-groups update-names-vserver_vserver_name_-display-failed-only true'
업데이트에 대한 모든 상태 정보를 표시하지 않습니다	'vserver cifs users-and-groups update-names-vserver_vserver_name_-suppress-all-output TRUE'

### 3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 스토리지 가상 머신(SVM, 이전의 Vserver) VS1 과 관련된 도메인 사용자 및 그룹의 이름을 업데이트합니다. 마지막 업데이트 시 업데이트해야 할 종속 이름 체인이 있습니다.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:           EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:           EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

로컬 권한을 관리합니다

로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다

권한을 추가하여 로컬 또는 도메인 사용자 또는 그룹의 사용자 권한을 관리할 수 있습니다. 추가된 권한은 이러한 개체에 할당된 기본 권한을 재정의합니다. 사용자 또는 그룹에 있는 권한을 사용자 지정할 수 있으므로 보안이 강화됩니다.

시작하기 전에

권한을 추가할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

객체에 권한을 추가하면 해당 사용자 또는 그룹에 대한 기본 권한이 재정의됩니다. 권한을 추가해도 이전에 추가한 권한은 제거되지 않습니다.

로컬 또는 도메인 사용자 또는 그룹에 권한을 추가할 때는 다음 사항을 염두에 두어야 합니다.

- 하나 이상의 권한을 추가할 수 있습니다.
- 도메인 사용자 또는 그룹에 권한을 추가할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다.

ONTAP가 도메인 컨트롤러에 연결할 수 없는 경우 명령이 실패할 수 있습니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에 하나 이상의 권한을 추가합니다. 'vserver cifs users-and-groups privilege add-privilege-vserver\_name\_-user-or-group-name name name-Privileges\_Privilege\_[,...]'
2. 원하는 권한이 객체에 적용되었는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 사용자 " cifs\_server\sue ""에 "seTcbPrivilege" 및 "setTakeOwnershipPrivilege" 권한을 추가합니다1.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거합니다

권한을 제거하여 로컬 또는 도메인 사용자 또는 그룹에 대한 사용자 권한을 관리할 수 있습니다. 이렇게 하면 사용자와 그룹이 보유한 최대 권한을 사용자 지정할 수 있으므로 보안이 강화됩니다.

## 시작하기 전에

권한을 제거할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

## 이 작업에 대해

로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거할 때는 다음 사항을 염두에 두어야 합니다.

- 하나 이상의 권한을 제거할 수 있습니다.
- 도메인 사용자 또는 그룹에서 권한을 제거할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다.

ONTAP가 도메인 컨트롤러에 연결할 수 없는 경우 명령이 실패할 수 있습니다.

## 단계

1. 로컬 또는 도메인 사용자 또는 그룹에서 하나 이상의 권한을 제거합니다. 'vserver cifs users-and-groups privilege remove-privilege-vserver\_name\_-user-or-group-name\_name\_-Privileges\_Privilege\_[,...]'
2. 원하는 권한이 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_' 객체에서 제거되었는지 확인합니다

## 예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 사용자 " cifs\_server\sue "(cifs\_server\sue ")에서 "seTcbPrivilege' 및 "setegenershipPrivilege" 권한을 제거합니다1.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        -
```

로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정합니다

로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정할 수 있습니다. 이 기능은 로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 수정한 후 해당 수정 사항이 더 이상 필요 또는 필요하지 않을 때 유용합니다.

## 이 작업에 대해

로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 재설정하면 해당 개체에 대한 권한 항목이 제거됩니다.

## 단계

1. 로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 재설정합니다. 'vserver cifs users-and-groups privilege reset-privilege-vserver\_name\_-user-or-group-name\_name\_'
2. 객체에 대한 권한이 재설정되었는지 확인합니다. 'vserver cifs users-and-groups privilege show -vserver\_vserver\_name\_-user-or-group-name\_name\_'

## 예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 에서 사용자 "cifs\_server\sue"에 대한 권한을 재설정합니다. 기본적으로 일반 사용자는 자신의 계정과 연결된 권한이 없습니다.

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

다음 예제에서는 "BUILTIN\Administrators" 그룹에 대한 권한을 다시 설정하여 권한 항목을 효과적으로 제거합니다.

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        BUILTIN\Administrators  SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

권한 재정의에 대한 정보를 표시합니다

도메인 또는 로컬 사용자 계정 또는 그룹에 할당된 사용자 지정 권한에 대한 정보를 표시할 수 있습니다. 이 정보를 통해 원하는 사용자 권한이 적용되는지 여부를 확인할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	이 명령을 입력하십시오...
SVM(스토리지 가상 시스템)의 모든 도메인 및 로컬 사용자 및 그룹에 대한 사용자 지정 권한	'vserver cifs users-and-groups privilege show -vserver_vserver_name_'
SVM에서 특정 도메인 또는 로컬 사용자 및 그룹에 대한 사용자 지정 권한	'vserver cifs users-and-groups 권한 표시 -vserver_vserver_name_-user-or-group-name_name_'

이 명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

예

다음 명령을 실행하면 SVM VS1에 대한 로컬 또는 도메인 사용자 및 그룹과 명시적으로 연결된 모든 권한이 표시됩니다.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1          CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

## 우회 통과 검사를 구성합니다

### 우회 횡단 검사 개요 구성

통과 확인 무시 사용자 권한(`_privilege_`라고도 함)은 사용자가 이동 중인 디렉터리에 대한 권한이 없더라도 경로 내의 모든 디렉터리를 파일로 이동할 수 있는지 여부를 결정합니다. 통과 확인을 허용 또는 허용하지 않을 경우 어떤 일이 발생하는지, 그리고 SVM(스토리지 가상 시스템)에서 사용자에게 대한 통과 확인을 건너뛰도록 구성하는 방법을 이해해야 합니다.

우회 통과 확인을 허용 또는 허용하지 않을 때 발생하는 현상

- 허용되는 경우 사용자가 파일에 액세스하려고 할 때 ONTAP는 파일에 대한 액세스 허용 또는 거부 여부를 결정할 때 중간 디렉터리에 대한 통과 권한을 확인하지 않습니다.
- 허용되지 않는 경우 ONTAP는 파일 경로에 있는 모든 디렉터리에 대해 트래버스(실행) 권한을 확인합니다.

중간 디렉터리에 ""X""(통과 권한)이 없으면 ONTAP는 해당 파일에 대한 액세스를 거부합니다.

### 우회 통과 검사를 구성합니다

ONTAP CLI를 사용하거나 이 사용자 권한으로 Active Directory 그룹 정책을 구성하여 통과 통과 확인 바이패스를 구성할 수 있습니다.

'eChangeNotifyPrivilege' 권한은 사용자가 횡단 확인을 우회할 수 있는지 여부를 제어합니다.

- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에 추가하면 통과 확인을 건너뛸 수 있습니다.
- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에서 제거하면 통과 확인을 건너뛸 수 없습니다.

기본적으로 SVM의 다음 BUILTIN 그룹에는 횡단 확인을 건너뛸 수 있는 권한이 있습니다.

- 'BUILTIN\Administrators'
- 'BUILTIN\Power Users'
- 'BUILTIN\Backup Operators'
- 'BUILTIN\Users'
- '모든 사람'

이러한 그룹 중 하나의 구성원이 통과 확인을 건너뛰도록 허용하지 않으려면 그룹에서 이 권한을 제거해야 합니다.

CLI를 사용하여 SVM에서 로컬 SMB 사용자 및 그룹에 대한 통과 검사를 구성할 때 다음 사항을 염두에 두어야 합니다.

- 사용자 지정 로컬 또는 도메인 그룹의 구성원이 통과 확인을 건너뛰도록 하려면 해당 그룹에 'eChangeNotifyPrivilege' 권한을 추가해야 합니다.
- 개별 로컬 또는 도메인 사용자가 횡단 검사를 무시하도록 허용하고 해당 권한이 있는 그룹의 구성원이 아닌 경우 해당 사용자 계정에 'eChangeNotifyPrivilege' 권한을 추가할 수 있습니다.
- 언제든지 'ChangeNotifyPrivilege' 권한을 제거하여 로컬 또는 도메인 사용자 또는 그룹에 대한 통과 확인을 사용하지 않도록 설정할 수 있습니다.



지정된 로컬 또는 도메인 사용자 또는 그룹에 대한 우회 트래버스 검사를 비활성화하려면 "Everyone" 그룹에서 'ChangeNotifyPrivilege' 권한도 제거해야 합니다.

#### 관련 정보

[사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다](#)

[디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다](#)

[볼륨에서 SMB 파일 이름 변환에 대한 문자 매핑을 구성합니다](#)

[SMB 공유 액세스 제어 목록을 생성합니다](#)

[Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다](#)

[지원되는 권한 목록입니다](#)

[로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다](#)

[사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다](#)

사용자가 이동 중인 디렉토리에 대한 사용 권한이 없더라도 경로 내의 모든 디렉토리를 통과할 수 있도록 하려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하면 됩니다. 기본적으로 사용자는 디렉터리 통과 확인을



건너뛸 수 있습니다.

시작하기 전에

- SVM에 SMB 서버가 있어야 합니다.
- 로컬 사용자 및 그룹 SMB 서버 옵션을 활성화해야 합니다.
- 'eChangeNotifyPrivilege' 권한을 추가할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

도메인 사용자 또는 그룹에 권한을 추가할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하여 통과 확인을 사용하지 않도록 설정합니다. 'vserver cifs users-and-groups privilege add-privilege\_vserver\_name\_-user-or-group-name\_name\_-Privileges SeChangeNotifyPrivilege'

'-user-or-group-name' 매개 변수의 값은 로컬 사용자 또는 그룹 또는 도메인 사용자 또는 그룹입니다.

2. 지정된 사용자 또는 그룹이 통과 확인 생략 기능을 사용하도록 설정했는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_'

예

다음 명령을 사용하면 "Example\eng" 그룹에 속한 사용자가 'seChangeNotifyPrivilege' 권한을 그룹에 추가하여 디렉터리 통과 확인을 건너뛸 수 있습니다.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng             SeChangeNotifyPrivilege
```

관련 정보

[사용자 또는 그룹이 디렉터리 트래버스 검사를 건너뛰는 것을 허용하지 않습니다](#)

디렉터리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다

사용자가 이동 중인 디렉토리에 대한 권한이 없기 때문에 경로 내의 모든 디렉토리를 이동하지 않으려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에서 'seChangeNotifyPrivilege' 권한을 제거할 수 있습니다.

시작하기 전에

권한을 제거할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

도메인 사용자 또는 그룹에서 권한을 제거할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

#### 단계

1. 통과 확인 무시 허용 안 함: 'vserver cifs users-and-groups privilege remove-privilege-vserver\_vserver\_name\_-user-or-group-name\_name\_-Privileges SeChangeNotifyPrivilege'  
  
이 명령은 '-user-or-group-name\_name\_' 매개 변수 값으로 지정한 로컬 또는 도메인 사용자 또는 그룹에서 'seChangeNotifyPrivilege' 권한을 제거합니다.
2. 지정된 사용자 또는 그룹이 통과 확인을 사용하지 않도록 설정했는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_'

#### 예

다음 명령을 실행하면 디렉토리 트래버스 검사를 거치지 않고 "example\eng" 그룹에 속한 사용자가 사용할 수 없습니다.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              -
```

#### 관련 정보

[사용자 또는 그룹이 디렉토리 통과 확인을 생략하도록 허용합니다](#)

### 파일 보안 및 감사 정책에 대한 정보를 표시합니다

파일 보안 및 감사 정책 개요에 대한 정보를 표시합니다

SVM(스토리지 가상 머신)의 볼륨 내에 포함된 파일 및 디렉토리의 파일 보안에 대한 정보를 표시할 수 있습니다. FlexVol 볼륨의 감사 정책에 대한 정보를 표시할 수 있습니다. 구성된 경우 FlexVol 볼륨의 저장소 수준 액세스 가드 및 동적 액세스 제어 보안 설정에 대한 정보를 표시할 수 있습니다.

#### 파일 보안에 대한 정보 표시

다음 보안 스타일을 사용하여 볼륨 및 Qtree(FlexVol 볼륨의 경우) 내에 포함된 데이터에 적용되는 파일 보안에 대한 정보를 표시할 수 있습니다.

- NTFS입니다
- Unix
- 혼합

감사 정책에 대한 정보 표시

다음 NAS 프로토콜을 통해 FlexVol 볼륨의 액세스 이벤트를 감사하기 위한 감사 정책에 대한 정보를 표시할 수 있습니다.

- SMB(모든 버전)
- NFSv4.x

스토리지 레벨 액세스 가드(슬래그) 보안에 대한 정보 표시

스토리지 레벨 액세스 가드 보안은 FlexVol 볼륨 및 qtree 개체에 다음 보안 스타일로 적용할 수 있습니다.

- NTFS입니다
- 혼합
- UNIX(볼륨을 포함하는 SVM에서 CIFS 서버가 구성된 경우)

**DAC(Dynamic Access Control)** 보안에 대한 정보 표시

동적 액세스 제어 보안은 다음 보안 스타일을 사용하여 FlexVol 볼륨 내의 개체에 적용할 수 있습니다.

- NTFS입니다
- 혼합(오브젝트에 NTFS 유효 보안이 있는 경우)

관련 정보

[Storage-Level Access Guard를 사용하여 파일 액세스 보호](#)

[Storage-Level Access Guard에 대한 정보 표시](#)

**NTFS** 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

NTFS 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안 스타일, 적용되는 권한, DOS 속성 정보 등)를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용하므로 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.
- ACL 출력은 NTFS 보안이 설정된 파일 및 폴더에 대해 표시됩니다.
- 볼륨 루트 또는 qtree에서 Storage-Level Access Guard 보안을 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 ACL과 Storage-Level Access Guard ACL이 모두

표시될 수 있습니다.

- 또한 동적 액세스 제어가 지정된 파일 또는 디렉터리 경로에 대해 구성된 경우 이 출력에는 동적 액세스 제어 ACE에 대한 정보도 표시됩니다.

#### 단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver_vserver_name_-path_path_'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver_vserver_name_-path_path_-expand-mask true'

#### 예

다음 예제는 SVM VS1 경로의 /vol4" 보안 정보를 보여줍니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

                Vserver: vs1
                File Path: /vol4
        File Inode Number: 64
                Security Style: ntfs
        Effective Style: ntfs
                DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
                Unix User Id: 0
                Unix Group Id: 0
                Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
                ACLs: NTFS Security Descriptor
                        Control:0x8004
                        Owner:BUILTIN\Administrators
                        Group:BUILTIN\Administrators
                        DACL - ACEs
                        ALLOW-Everyone-0x1f01ff
                        ALLOW-Everyone-0x10000000-
```

OI|CI|IO

다음 예에서는 SVM VS1 경로의 /data/engineering에 대한 확장된 마스크와 함께 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
```

```
/data/engineering -expand-mask true
```

```

    Vserver: vs1
    File Path: /data/engineering
    File Inode Number: 5544
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: 0x10
    ....0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004
```

```

    1... .... = Self Relative
    .0.. .... = RM Control Valid
    ..0. .... = SACL Protected
    ...0 .... = DACL Protected
    .... 0... = SACL Inherited
    .... .0.. = DACL Inherited
    .... ..0. = SACL Inherit Required
    .... ...0 = DACL Inherit Required
    .... .... ..0. = SACL Defaulted
    .... .... ...0 = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted
```

```

    Owner:BUILTIN\Administrators
    Group:BUILTIN\Administrators
    DACL - ACEs
```

```
    ALLOW-Everyone-0x1f01ff
```

```
    0... .... =
```

```
Generic Read
```

Generic Write	.0.. .....	=
Generic Execute	..0. ....	=
Generic All	...0 .....	=
System Security	.... ...0 .....	=
Synchronize	.... ....1 .....	=
Write Owner	.... ....1... .....	=
Write DAC	.... ....1... .....	=
Read Control	.... ....1. ....	=
Delete	.... ....1 .....	=
Write Attributes	.... ....1 .....	=
Read Attributes	.... ....1... .....	=
Delete Child	.... ....1... .....	=
Execute	.... ....1. ....	=
Write EA	.... ....1 .....	=
Read EA	.... ....1... .....	=
Append	.... ....1... .....	=
Write	.... ....1. ....	=
Read	.... ....1 .....	=
ALLOW-Everyone-0x10000000-OI CI IO		
Generic Read	0... .....	=
Generic Write	.0.. ....	=
Generic Execute	..0. ....	=
Generic All	...1 .....	=

System Security	.....0.....	=
Synchronize	.....0.....	=
Write Owner	.....0.....	=
Write DAC	.....0.....	=
Read Control	.....0.....	=
Delete	.....0.....	=
Write Attributes	.....0.....	=
Read Attributes	.....0.....	=
Delete Child	.....0.....	=
Execute	.....0.....	=
Write EA	.....0.....	=
Read EA	.....0.....	=
Append	.....0.....	=
Write	.....0.....	=
Read	.....0.....	=

다음 예에서는 SVM VS1 에서 경로 '/datavol1'이 있는 볼륨에 대한 Storage-Level Access Guard 보안 정보를 비롯한 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner:BUILTIN\Administrators
          Group:BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

관련 정보

[혼합 보안 형식 볼륨의 파일 보안에 대한 정보 표시](#)

[UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보 표시](#)



혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다

보안 스타일 및 효과적인 보안 스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등 혼합 보안 스타일 볼륨에 대한 파일 및 디렉터리 보안에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- 혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉터리 등 UNIX 파일 권한을 사용하는 일부 파일 및 폴더가 포함될 수 있습니다.
- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 있을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉터리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 UNIX 파일 사용 권한과 Storage-Level Access Guard ACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉터리 경로에 동적 액세스 제어기가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예에서는 SVM VS1 경로 '/projects'에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다. 이 혼합 보안 방식 경로에는 UNIX의 효과적인 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path  
/projects -expand-mask true
```

```
        Vserver: vs1  
        File Path: /projects  
File Inode Number: 78  
    Security Style: mixed  
    Effective Style: unix  
    DOS Attributes: 10  
DOS Attributes in Text: ----D---  
Expanded Dos Attributes: 0x10  
    ...0 .... = Offline  
    .... ..0. .... = Sparse  
    .... .... 0... .... = Normal  
    .... .... ..0. .... = Archive  
    .... .... ...1 .... = Directory  
    .... .... .... .0.. = System  
    .... .... .... ..0. = Hidden  
    .... .... .... ...0 = Read Only  
        Unix User Id: 0  
        Unix Group Id: 1  
        Unix Mode Bits: 700  
Unix Mode Bits in Text: rwx-----  
        ACLs: -
```

다음 예제는 SVM VS1 경로 '/data'에 대한 보안 정보를 보여줍니다. 이 혼합 보안 방식 경로에는 NTFS의 효과적인 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에 있는 볼륨에 대한 보안 정보를 표시합니다. 이러한 혼합 보안 유형의 최상위 수준에는 UNIX의 효과적인 보안이 있습니다. 이 볼륨에는 Storage-Level Access Guard 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
```

#### 관련 정보

[NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보 표시](#)

[UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보 표시](#)

**UNIX** 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

UNIX 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안 스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등)를 표시할 수 있습니다. 결과를

사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 디렉토리 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 모드 비트 또는 NFSv4 ACL 중 하나의 UNIX 파일 권한만 사용합니다.
- NFSv4 보안이 설정된 파일 및 폴더에 대해서만 ACL 출력이 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉토리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- NFSv4 보안 설명자의 경우 ACL 출력의 소유자 및 그룹 출력 필드는 적용되지 않습니다.

NTFS 보안 설명자에만 의미가 있습니다.

- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver_vserver_name_-path_path_'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver_vserver_name_-path_path_-expand-mask true'

예

다음 예제는 SVM VS1 경로의 / home 경로에 대한 보안 정보를 표시합니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

        Vserver: vs1
        File Path: /home
        File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
            Unix User Id: 0
            Unix Group Id: 1
            Unix Mode Bits: 700
        Unix Mode Bits in Text: rwx-----
            ACLs: -
```

다음 예에서는 SVM VS1 경로의 /home 경로에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

        Vserver: vs1
        File Path: /home
        File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: 0x10
            ...0 .... .... = Offline
            .... ..0. .... = Sparse
            .... .... 0... .... = Normal
            .... .... ..0. .... = Archive
            .... .... ...1 .... = Directory
            .... .... .... .0.. = System
            .... .... .... ..0. = Hidden
            .... .... .... ...0 = Read Only
            Unix User Id: 0
            Unix Group Id: 1
            Unix Mode Bits: 700
        Unix Mode Bits in Text: rwx-----
            ACLs: -
```

## NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보 표시

### 혼합 보안 형식 볼륨의 파일 보안에 대한 정보 표시

CLI를 사용하여 **FlexVol** 볼륨의 **NTFS** 감사 정책에 대한 정보를 표시합니다

FlexVol 볼륨에서 보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 시스템 액세스 제어 목록에 대한 정보를 포함하여 NTFS 감사 정책에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 폴더의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 감사 정책에 NTFS SACL(시스템 액세스 제어 목록)만 사용합니다.
- NTFS 효과적인 보안이 적용된 혼합 보안 스타일 볼륨의 파일과 폴더에 NTFS 감사 정책이 적용될 수 있습니다.

혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 포함될 수 있으며 NTFS SACL이 포함될 수도 있고 포함되지 않을 수도 있습니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 및 폴더 NFSv4 SACL 및 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어기가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.
- NTFS 유효 보안이 있는 파일 및 폴더에 대한 보안 정보를 표시할 때 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.

NTFS 보안 스타일 파일 및 폴더는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용합니다.

- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.

단계

1. 파일 및 디렉터리 감사 정책 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'

정보를 표시하려면...	다음 명령을 입력합니다...
를 참조하십시오	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예에서는 SVM VS1 경로의 /Corp 경로에 대한 감사 정책 정보를 표시합니다. 경로에 NTFS 유효 보안이 있습니다. NTFS 보안 설명자는 성공 및 성공/실패 SACL 항목을 모두 포함합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACEs
      ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
      SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
      ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
      ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
      ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

다음 예제는 SVM VS1 경로의 /datavol1 경로에 대한 감사 정책 정보를 표시합니다. 이 경로에는 일반 파일 및 폴더 SACL과 Storage-Level Access Guard SACL이 모두 포함됩니다.



```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

        Vserver: vs1
        File Path: /datavol1
        File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
            Unix User Id: 0
            Unix Group Id: 0
            Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

        Storage-Level Access Guard security
        SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
        SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

CLI를 사용하여 **FlexVol** 볼륨에서 **NFSv4** 감사 정책에 대한 정보를 표시합니다

보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 SACL(시스템 액세스 제어 목록)에 대한 정보를 포함하여 ONTAP CLI를 사용하여 FlexVol 볼륨에서 NFSv4 감사 정책에 대한

정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 디렉토리의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 감사 정책에 NFSv4 SACL만 사용합니다.
- UNIX 보안 스타일의 혼합 보안 스타일 볼륨에 있는 파일과 디렉토리에는 NFSv4 감사 정책이 적용될 수 있습니다.

혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준은 UNIX 또는 NTFS의 유효 보안을 가질 수 있으며 NFSv4 SACL을 포함하거나 포함하지 않을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 NFSv4 파일 및 디렉터리 SACL과 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예제는 SVM VS1 경로 /lab에 대한 보안 정보를 보여 줍니다. 이 UNIX 보안 스타일 경로에는 NFSv4 SACL이 있습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab
```

```

    Vserver: vs1
    File Path: /lab
    File Inode Number: 288
    Security Style: unix
    Effective Style: unix
    DOS Attributes: 11
    DOS Attributes in Text: ----D--R
    Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 0
    Unix Mode Bits in Text: -----
        ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
                SUCCESSFUL-S-1-520-0-0xf01ff-SA
                FAILED-S-1-520-0-0xf01ff-FA
            DACL - ACEs
                ALLOW-S-1-520-1-0xf01ff
```

파일 보안 및 감사 정책에 대한 정보를 표시하는 방법

와일드카드 문자(\*)를 사용하여 지정된 경로 또는 루트 볼륨 아래에 있는 모든 파일 및 디렉토리의 파일 보안 및 감사 정책에 대한 정보를 표시할 수 있습니다.

와일드카드 문자(\*)는 모든 파일 및 디렉토리의 정보를 표시할 아래의 지정된 디렉터리 경로의 마지막 하위 구성 요소로 사용할 수 있습니다. "" \* ""로 명명된 특정 파일이나 디렉토리의 정보를 표시하려면 큰따옴표("") 안에 전체 경로를 제공해야 합니다.

예

와일드카드 문자를 사용하여 다음 명령을 실행하면 SVM VS1 경로의 '/1/' 아래에 있는 모든 파일 및 디렉토리에 대한 정보가 표시됩니다.

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

다음 명령을 실행하면 SVM VS1 의 path '/vol1/a' 아래에 " \*"로 명명된 파일의 정보가 표시됩니다. 경로는 큰따옴표(")로 묶습니다.

```
cluster::> vservers security file-directory show -vservers vs1 -path  
"/vol1/a/*"
```

```
      Vserver: vs1  
      File Path: "/vol1/a/*"  
      Security Style: mixed  
      Effective Style: unix  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: -  
      Unix User Id: 1002  
      Unix Group Id: 65533  
      Unix Mode Bits: 755  
      Unix Mode Bits in Text: rwxr-xr-x  
      ACLs: NFSV4 Security Descriptor  
      Control:0x8014  
      SACL - ACEs  
      AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
      DACL - ACEs  
      ALLOW-EVERYONE@-0x1f00a9-FI|DI  
      ALLOW-OWNER@-0x1f01ff-FI|DI  
      ALLOW-GROUP@-0x1200a9-IG
```

## CLI를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다

CLI 개요를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다

CLI를 사용하여 스토리지 가상 시스템(SVM)에서 NTFS 파일 보안, NTFS 감사 정책 및 스토리지 레벨 액세스 가드를 관리할 수 있습니다.

SMB 클라이언트 또는 CLI를 사용하여 NTFS 파일 보안 및 감사 정책을 관리할 수 있습니다. 그러나 CLI를 사용하여 파일 보안 및 감사 정책을 구성하면 원격 클라이언트를 사용하여 파일 보안을 관리할 필요가 없습니다. CLI를 사용하면 단일 명령을 사용하여 여러 파일과 폴더에 보안을 적용하는 데 걸리는 시간을 크게 줄일 수 있습니다.

ONTAP에서 SVM 볼륨에 적용한 또 다른 보안 계층인 스토리지 레벨 액세스 가드를 구성할 수 있습니다. Storage-Level Access Guard는 모든 NAS 프로토콜에서 Storage-Level Access Guard가 적용되는 스토리지 객체에 대한 액세스에 적용됩니다.

스토리지 레벨 액세스 가드는 ONTAP CLI에서만 구성 및 관리할 수 있습니다. SMB 클라이언트에서 스토리지 수준 액세스 가드 설정을 관리할 수 없습니다. 또한 NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다. 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 액세스 가드 보안을 취소할 수 없습니다. 따라서 Storage-Level Access Guard는 스토리지 관리자가 독립적으로 설정하고 관리하는 데이터 액세스를 위한 추가 보안 계층을 제공합니다.



스토리지 레벨 액세스 가드에 대해 NTFS 액세스 권한만 지원되지만, ONTAP은 UNIX 사용자가 볼륨을 소유하는 SVM에서 Windows 사용자에게 매핑될 경우 스토리지 레벨 액세스 가드가 적용되는 볼륨의 데이터에 대해 NFS에 대한 액세스를 위한 보안 검사를 수행할 수 있습니다.

## NTFS 보안 스타일 볼륨

NTFS 보안 스타일 볼륨 및 Qtree에 포함된 모든 파일 및 폴더는 NTFS의 효율적인 보안을 사용합니다. "vserver security file-directory" 명령 제품군을 사용하여 NTFS 보안 스타일 볼륨에 다음 유형의 보안을 구현할 수 있습니다.

- 볼륨에 포함된 파일 및 폴더에 대한 파일 권한 및 감사 정책
- 볼륨에 대한 스토리지 레벨 액세스 가드 보안

## 혼합 보안 형식 볼륨

혼합 보안 스타일 볼륨 및 qtree에는 UNIX의 효과적인 보안이 있는 일부 파일과 폴더가 포함될 수 있으며, 모드 비트 또는 NFSv4.x ACL 및 NFSv4.x 감사 정책, NTFS 효과적인 보안이 설정된 일부 파일 및 폴더, NTFS 파일 권한 및 감사 정책을 사용하는 일부 파일 및 폴더가 포함될 수 있습니다. 'vserver security file-directory' 명령 제품군을 사용하여 혼합 보안 스타일 데이터에 다음 유형의 보안을 적용할 수 있습니다.

- 혼합 볼륨 또는 qtree에서 NTFS 유효 보안 유형을 사용하는 파일 및 폴더에 대한 파일 권한 및 감사 정책
- 스토리지 레벨 액세스 NTFS 및 UNIX의 효율적인 보안 방식으로 볼륨에 대한 보호

## Unix 보안 스타일 볼륨

UNIX 보안 스타일 볼륨 및 qtree에는 UNIX 유효 보안(모드 비트 또는 NFSv4.x ACL)이 있는 파일 및 폴더가 포함되어 있습니다. UNIX 보안 스타일 볼륨에 보안을 구현하기 위해 'vserver security file-directory' 명령 제품군을 사용하려면 다음 사항을 염두에 두어야 합니다.

- "vserver security file-directory" 명령 제품군은 UNIX 보안 스타일 볼륨 및 qtree에서 UNIX 파일 보안 및 감사 정책을 관리하는 데 사용할 수 없습니다.
- SVM과 타겟 볼륨에 CIFS 서버가 포함된 경우 "vserver security file-directory" 명령 제품군을 사용하여 UNIX 보안 스타일 볼륨에서 Storage-Level Access Guard를 구성할 수 있습니다.

## 관련 정보

[파일 보안 및 감사 정책에 대한 정보를 표시합니다](#)

[CLI를 사용하여 NTFS 파일 및 폴더에 파일 보안을 구성하고 적용합니다](#)

[CLI를 사용하여 NTFS 파일 및 폴더에 감사 정책을 구성하고 적용합니다](#)

[Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다](#)

## CLI를 사용하여 파일 및 폴더 보안을 설정하는 사용 사례

원격 클라이언트의 개입 없이 로컬로 파일 및 폴더 보안을 적용 및 관리할 수 있으므로 많은 수의 파일 또는 폴더에 대해 대량 보안을 설정하는 데 걸리는 시간을 크게 줄일 수 있습니다.

CLI를 사용하여 다음과 같은 사용 사례에서 파일 및 폴더 보안을 설정할 수 있습니다.

- 홈 디렉토리의 파일 스토리지와 같은 대규모 엔터프라이즈 환경에 있는 파일의 스토리지

- 데이터 마이그레이션
- Windows 도메인 변경
- NTFS 파일 시스템 전반에 걸쳐 파일 보안 및 감사 정책 표준화

CLI를 사용하여 파일 및 폴더 보안을 설정할 때의 제한 사항

CLI를 사용하여 파일 및 폴더 보안을 설정할 때 특정 제한 사항을 알고 있어야 합니다.

- 'vserver security file-directory' 명령 제품군은 NFSv4 ACL 설정을 지원하지 않습니다.

NTFS 보안 설명자는 NTFS 파일 및 폴더에만 적용할 수 있습니다.

보안 설명자를 사용하여 파일 및 폴더 보안을 적용하는 방법

보안 설명자는 사용자가 파일 및 폴더에 대해 수행할 수 있는 작업과 사용자가 파일 및 폴더에 액세스할 때 감사할 작업을 결정하는 액세스 제어 목록을 포함합니다.

- \* 권한 \*

권한은 개체의 소유자가 허용하거나 거부하고 개체(사용자, 그룹 또는 컴퓨터 개체)가 지정된 파일이나 폴더에서 수행할 수 있는 작업을 결정합니다.

- \* 보안 설명자 \*

보안 설명자는 파일 또는 폴더와 관련된 권한을 정의하는 보안 정보가 포함된 데이터 구조입니다.

- \* ACL(액세스 제어 목록) \*

액세스 제어 목록은 보안 설명자가 적용된 파일 또는 폴더에서 사용자, 그룹 또는 컴퓨터 개체가 수행할 수 있는 작업에 대한 정보를 포함하는 보안 설명자에 포함된 목록입니다. 보안 설명자는 다음 두 가지 유형의 ACL을 포함할 수 있습니다.

- DACL(임의 액세스 제어 목록)
- 시스템 액세스 제어 목록(SACL)

- \* DACL(임의 액세스 제어 목록) \*

DACL에는 파일 또는 폴더에 대한 작업을 수행할 수 있는 액세스가 허용 또는 거부된 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. DACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- \* 시스템 액세스 제어 목록(SACL) \*

SACL에는 성공 또는 실패 감사 이벤트가 기록되는 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. SACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- \* ACE(액세스 제어 항목) \*

ACE는 DACL 또는 SACL의 개별 항목입니다.

- DACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에 대해 허용 또는 거부된 액세스 권한을

지정합니다.

- SACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에서 수행하는 지정된 작업을 감사할 때 기록할 성공 또는 실패 이벤트를 지정합니다.

• \* 사용 권한 상속 \*

권한 상속에서는 보안 설명자에 정의된 권한이 부모 개체에서 개체로 전파되는 방법을 설명합니다. 상속 가능한 권한만 자식 개체에서 상속합니다. 상위 객체에 대한 권한을 설정할 때 폴더, 하위 폴더, 파일이 이 폴더에 적용, 하위 폴더, 파일 등을 통해 해당 항목을 상속할 수 있는지 여부를 결정할 수 있습니다.

## 관련 정보

["SMB 및 NFS 감사 및 보안 추적"](#)

[CLI를 사용하여 NTFS 파일 및 폴더에 감사 정책 구성 및 적용](#)

**SVM** 재해 복구 대상에서 로컬 사용자 또는 그룹을 사용하는 파일 디렉토리 정책을 적용하기 위한 지침

파일 디렉토리 정책 구성에서 보안 설명자나 DACL 또는 SACL 항목의 로컬 사용자 또는 그룹을 사용하는 경우 ID 폐기 구성의 SVM(Storage Virtual Machine) 재해 복구 대상에 파일 디렉토리 정책을 적용하기 전에 염두에 두어야 할 몇 가지 지침이 있습니다.

소스 클러스터의 소스 SVM이 소스 SVM에서 데이터 및 구성을 소스 SVM에서 타겟 클러스터의 대상 SVM으로 복제하는 SVM을 위한 재해 복구 구성을 구성할 수 있습니다.

SVM 재해 복구의 두 가지 유형 중 하나를 설정할 수 있습니다.

- ID가 보존됩니다

이 구성에서는 SVM과 CIFS 서버의 ID가 보존됩니다.

- ID가 삭제되었습니다

이 구성에서는 SVM과 CIFS 서버의 ID가 유지되지 않습니다. 이 시나리오에서는 대상 SVM의 SVM 및 CIFS 서버의 이름이 소스 SVM의 SVM 및 CIFS 서버 이름과 다릅니다.

## ID 폐기 구성에 대한 지침

로컬 사용자, 그룹 및 권한 구성이 포함된 SVM 소스의 경우 ID가 폐기된 구성에서 SVM 대상의 CIFS 서버 이름과 일치하도록 로컬 도메인(로컬 CIFS 서버 이름)의 이름을 변경해야 합니다. 예를 들어, 소스 SVM 이름이 ""VS1""이고 CIFS 서버 이름이 ""CIFS1""이고 대상 SVM 이름이 ""VS1\_DST""이고 CIFS 서버 이름이 ""CIFS1\_DST""인 경우 로컬 사용자 ""CIFS1\user1""의 로컬 도메인 이름이 ""FS1""으로 자동 변경됩니다.



```
cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1_dst
```

Vsriver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in
administrator account			
vs1	CIFS1\user1	-	-

```
cluster1dst::> vsriver cifs users-and-groups local-user show -vsriver vs1_dst
```

Vsriver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in
administrator account			
vs1_dst	CIFS1_DST\user1	-	-

로컬 사용자 및 그룹 데이터베이스에서 로컬 사용자 및 그룹 이름이 자동으로 변경되더라도 파일 디렉토리 정책 구성('vsriver security file-directory' 명령 제품군을 사용하여 CLI에 구성된 정책)에서 로컬 사용자 또는 그룹 이름이 자동으로 변경되지 않습니다.

예를 들어, "vs1"의 경우 "-account" 매개 변수가 "CIFS1\user1"로 설정된 DACL 항목을 구성한 경우 대상의 CIFS 서버 이름을 반영하도록 대상 SVM에서 설정이 자동으로 변경되지 않습니다.

```
cluster1::> vsriver security file-directory ntfs dacl show -vsriver vs1
```

```
Vsriver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vsriver security file-directory ntfs dacl show -vsriver vs1_dst
```

```
Vsriver: vs1_dst
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
**CIFS1**\user1	allow	full-control	this-folder

CIFS 서버 이름을 대상 CIFS 서버 이름으로 수동으로 변경하려면 'vserver security file-directory modify' 명령을 사용해야 합니다.

계정 매개 변수가 포함된 파일 디렉토리 정책 구성 구성 요소입니다

로컬 사용자 또는 그룹을 포함할 수 있는 매개 변수 설정을 사용할 수 있는 세 가지 파일 디렉토리 정책 구성 구성 요소가 있습니다.

- 보안 설명자

필요에 따라 보안 설명자의 소유자와 보안 설명자의 소유자의 기본 그룹을 지정할 수 있습니다. 보안 설명자가 소유자 및 기본 그룹 항목에 대해 로컬 사용자 또는 그룹을 사용하는 경우, 계정 이름에 대상 SVM을 사용하도록 보안 설명자를 수정해야 합니다. 'vserver security file-directory NTFS modify' 명령을 사용하여 계정 이름을 필요에 따라 변경할 수 있습니다.

- DACL 항목

각 DACL 항목은 계정과 연결되어 있어야 합니다. 대상 SVM 이름을 사용하려면 로컬 사용자 또는 그룹 계정을 사용하는 모든 DACL을 수정해야 합니다. 기존 DACL 항목에 대한 계정 이름을 수정할 수 없으므로 보안 설명자에서 로컬 사용자 또는 그룹의 DACL 항목을 제거하고 수정된 대상 계정 이름으로 새 DACL 항목을 만든 다음 이러한 새 DACL 항목을 적절한 보안 설명자와 연결해야 합니다.

- SACL 항목

각 SACL 항목은 계정과 연결되어 있어야 합니다. 대상 SVM 이름을 사용하려면 로컬 사용자 또는 그룹 계정을 사용하는 SACL을 수정해야 합니다. 기존 SACL 항목에 대한 계정 이름을 수정할 수 없으므로 보안 설명자에서 로컬 사용자 또는 그룹을 가진 SACL 항목을 제거하고 수정된 대상 계정 이름으로 새 SACL 항목을 만든 다음 이러한 새 SACL 항목을 적절한 보안 설명자와 연결해야 합니다.

정책을 적용하기 전에 파일 디렉토리 정책 구성에 사용되는 로컬 사용자 또는 그룹을 변경해야 합니다. 그렇지 않으면 적용 작업이 실패합니다.

**CLI**를 사용하여 **NTFS** 파일 및 폴더에 파일 보안을 구성하고 적용합니다

**NTFS** 보안 설명자를 만듭니다

NTFS 보안 설명자(파일 보안 정책)를 생성하는 것은 NTFS ACL(액세스 제어 목록)을 구성하여 SVM(스토리지 가상 머신) 내에 있는 파일 및 폴더에 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결할 수 있습니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

오브젝트	액세스 유형입니다	액세스 권한	사용 권한을 적용할 위치입니다
BUILTIN\Administrators입니다	허용	모든 권한	폴더, 하위 폴더, 파일
BUILTIN\사용자	허용	모든 권한	폴더, 하위 폴더, 파일
작성자 소유자	허용	모든 권한	폴더, 하위 폴더, 파일
NT AUTHORITY\SYSTEM	허용	모든 권한	폴더, 하위 폴더, 파일

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다
- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

**NTFS DACL** 액세스 제어 항목을 **NTFS** 보안 설명자에 추가합니다

NTFS 보안 설명자에 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)를 추가하는 것은 파일이나 폴더에 NTFS ACL을 구성하고 적용하는 두 번째 단계입니다. 각 항목은 액세스가 허용되거나 거부된 개체를 식별하고 ACE에 정의된 파일 또는 폴더에 대해 개체가 수행할 수 있거나 수행할 수 없는 작업을 정의합니다.

이 작업에 대해

보안 설명자의 DACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 DACL이 포함된 경우 명령은 새 ACE를 DACL에 추가합니다. 보안 설명자에 DACL이 포함되어 있지 않으면 명령에서 DACL을 생성하고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정에 대해 허용 또는 거부할 권한을 지정하여 DACL 항목을 선택적으로 사용자 지정할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)



DACL 항목에 대한 권한을 지정하지 않으면 기본값은 "모든 권한"으로 설정됩니다.

선택적으로 상속 적용 방법을 지정하여 DACL 항목을 사용자 지정할 수 있습니다.

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

## 단계

1. 보안 설명자에 DACL 항목을 추가합니다. 'vserver security file -directory NTFS DACL add -vserver vserver\_name -ntfs -sd sd sd\_name -access -type {allow | deny} -account name\_or\_SID optional\_parameters'

```
'vserver security file-directory NTFS DACL add-NTFS-SD SD1-access-type deny-account domain\joe-rights full-control-apply-to this-folder-vserver-vs1'
```

2. DACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS DACL show -vserver vserver\_name -ntfs -sd sd sd\_name -access-type{allow|deny} -account name\_or\_SID'

```
'vserver security file-directory NTFS DACL show -vserver vs1-ntfs-sd SD1-access-type deny-account domain\joe'
```

```
Vserver: vs1
Security Descriptor Name: sd1
    Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
    Access Rights: full-control
Advanced Access Rights: -
    Apply To: this-folder
    Access Rights: full-control
```

## 보안 정책을 생성합니다

SVM에 대한 파일 보안 정책을 생성하는 것은 파일이나 폴더에 ACL을 구성 및 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각 작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

## 이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

## 단계

1. 'vserver security file-directory policy create-vserver vserver\_name-policy-name policy\_name' 보안 정책을 생성합니다

```
'vserver security file-directory policy create-policy-name policy1-vserver vs1'
```

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
```

보안 정책에 작업을 추가합니다

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 디렉터리 작업을 통해 적용된 ACL은 SMB 클라이언트 또는 ONTAP CLI를 통해 관리할 수 있습니다.

- 스토리지 레벨 액세스 가드 작업

지정된 볼륨에 Storage-Level Access Guard 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 스토리지 레벨 액세스 가드 작업을 통해 적용된 ACL은 ONTAP CLI를 통해서만 관리할 수 있습니다.

작업에는 파일(또는 폴더) 또는 파일 집합(또는 폴더)의 보안 구성에 대한 정의가 포함됩니다. 정책의 모든 작업은 경로로 고유하게 식별됩니다. 단일 정책 내에서 경로당 하나의 작업만 있을 수 있습니다. 정책에 중복된 작업 항목이 있을 수 없습니다.

정책에 작업 추가 지침:

- 정책당 최대 10,000개의 작업 항목이 있을 수 있습니다.
- 정책에는 하나 이상의 작업이 포함될 수 있습니다.

정책에 둘 이상의 작업이 포함될 수 있지만 파일 디렉터리 및 저장소 수준 액세스 가드 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉터리 작업이 포함되어야 합니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

추가 액세스 권한은 제공하지 않습니다.

보안 정책에 작업을 추가할 때 다음 네 가지 필수 매개 변수를 지정해야 합니다.

- SVM 이름
- 정책 이름입니다
- 경로
- 경로와 연결할 보안 설명자입니다

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 유형입니다

- 전파 모드
- 인덱스 위치
- 액세스 제어 유형입니다

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉토리 정책 작업 추가 - vs1 - vs1\_policy\_name -policy -name policy\_name -path path -NTFS-SD\_nameoptional\_parameters'

파일 디렉토리는 '-access-control' 파라미터의 기본값입니다. 파일 및 디렉터리 액세스 작업을 구성할 때 액세스 제어 유형을 지정하는 것은 선택 사항입니다.

'vserver security file-directory policy task add-vs1-policy-name policy1-path/home/dir1-security-type NTFS-NTFS-MODE propagate-NTFS-SD SD2-index-num 1-access-control file-directory'를 선택합니다

2. 정책 작업 구성을 확인합니다. 'vserver security file-directory policy task show -vserver vs1 -policy -name policy\_name -path path path'

'vserver security file-directory policy task show'를 선택합니다

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor Name					
-----	-----	-----	-----	-----	
1	/home/dir1	file-directory	ntfs	propagate	sd2

보안 정책을 적용합니다

파일 또는 폴더에 NTFS ACL을 생성하고 적용하는 마지막 단계는 SVM에 파일 보안 정책을 적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.



감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

단계

1. 보안 정책('vserver security file-directory apply-vserver vserver\_name -policy -name policy\_name')을 적용합니다

```
'vserver security file-directory apply-vserver vs1-policy-name policy1'
```

정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

보안 정책 작업을 모니터링합니다

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 'instance' 매개 변수를 사용해야 합니다.

단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vserver\_name'을 모니터링합니다

```
'vserver security file-directory job show -vserver vs1'
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

적용된 파일 보안을 확인합니다

파일 보안 설정을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 머신)의 파일 또는 폴더에 원하는 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

보안 설정을 확인할 파일과 폴더의 경로와 데이터가 포함된 SVM의 이름을 제공해야 합니다. 옵션 '-Expand-mask' 매개 변수를 사용하여 보안 설정에 대한 자세한 정보를 표시할 수 있습니다.

단계

1. 파일 및 폴더 보안 설정 표시: 'vserver security file-directory show -vserver vserver\_name -path path path[-expand-mask true]'

```
'vserver security file-directory show -vserver vs1-path/data/engineering-expand-mask true'
```

```

Vserver: vs1
    File Path: /data/engineering
File Inode Number: 5544
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

    1... .... = Self Relative
    .0.. .... = RM Control Valid
    ..0. .... = SACL Protected
    ...0 .... = DACL Protected
    .... 0... .... = SACL Inherited
    .... .0.. .... = DACL Inherited
    .... ..0. .... = SACL Inherit Required
    .... ...0 .... = DACL Inherit Required
    .... .... ..0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    0... .... =
Generic Read
    .0.. .... =
Generic Write

```



	..0. ....	=
Generic Execute	....0 ....	=
Generic All	.....0 ....	=
System Security	.....1 ....	=
Synchronize	.....1... ..	=
Write Owner	.....1... ..	=
Write DAC	.....1... ..	=
Read Control	.....1... ..	=
Delete	.....1... ..	=
Write Attributes	.....1... ..	=
Read Attributes	.....1... ..	=
Delete Child	.....1... ..	=
Execute	.....1... ..	=
Write EA	.....1... ..	=
Read EA	.....1... ..	=
Append	.....1... ..	=
Write	.....1... ..	=
Read	.....1... ..	=
ALLOW-Everyone-0x10000000-OI CI IO		
	0... ..	=
Generic Read	.0... ..	=
Generic Write	..0. ....	=
Generic Execute	...1 ....	=
Generic All	.....0 ....	=
System Security		

Synchronize	.....0.....	=
Write Owner	.....0.....	=
Write DAC	.....0.....	=
Read Control	.....0.....	=
Delete	.....0.....	=
Write Attributes	.....0.....	=
Read Attributes	.....0.....	=
Delete Child	.....0.....	=
Execute	.....0.....	=
Write EA	.....0.....	=
Read EA	.....0.....	=
Append	.....0.....	=
Write	.....0.....	=
Read	.....0.....	=

**CLI** 개요를 사용하여 **NTFS** 파일 및 폴더에 감사 정책을 구성하고 적용합니다

ONTAP CLI를 사용할 때 NTFS 파일 및 폴더에 감사 정책을 적용하려면 몇 가지 단계를 수행해야 합니다. 먼저 NTFS 보안 설명자를 만들고 보안 설명자에 SACL을 추가합니다. 그런 다음 보안 정책을 만들고 정책 작업을 추가합니다. 그런 다음 SVM(스토리지 가상 시스템)에 보안 정책을 적용합니다.

이 작업에 대해

보안 정책을 적용한 후 보안 정책 작업을 모니터링하고 적용된 감사 정책의 설정을 확인할 수 있습니다.



감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

관련 정보

[Storage-Level Access Guard를 사용하여 파일 액세스 보호](#)

CLI를 사용하여 파일 및 폴더 보안을 설정할 때의 제한 사항

보안 설명자를 사용하여 파일 및 폴더 보안을 적용하는 방법

"SMB 및 NFS 감사 및 보안 추적"

CLI를 사용하여 NTFS 파일 및 폴더에 파일 보안을 구성하고 적용합니다

**NTFS** 보안 설명자를 만듭니다

NTFS 보안 설명자 감사 정책을 생성하는 것은 SVM에 상주하는 파일 및 폴더에 NTFS ACL(액세스 제어 목록)을 구성 및 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결합니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

오브젝트	액세스 유형입니다	액세스 권한	사용 권한을 적용할 위치입니다
BUILTIN\Administrators입니다	허용	모든 권한	폴더, 하위 폴더, 파일
BUILTIN\사용자	허용	모든 권한	폴더, 하위 폴더, 파일
작성자 소유자	허용	모든 권한	폴더, 하위 폴더, 파일
NT AUTHORITY\SYSTEM	허용	모든 권한	폴더, 하위 폴더, 파일

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다
- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

단계

1. 고급 매개 변수를 사용하려면 권한 수준을 고급:'Set-Privilege Advanced'로 설정합니다
2. 보안 설명자:'vserver security file-directory NTFS create-vserver vs1-owner domain\joe' sd\_nameoptional\_parameters'를 생성합니다

'vserver security file-directory NTFS create-NTFS-SD SD1-vserver vs1-owner domain\joe'

3. 보안 설명자 구성이 올바른지 확인합니다. 'vserver security file-directory NTFS show -vserver vs1 -ntfs-sd sd1'

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. 고급 권한 수준인 경우 'Set-Privilege admin'으로 돌아갑니다

**NTFS SACL** 액세스 제어 항목을 **NTFS** 보안 설명자에 추가합니다

SACL(시스템 액세스 제어 목록) ACE(액세스 제어 항목)를 NTFS 보안 설명자에 추가하는 것은 SVM의 파일 또는 폴더에 대한 NTFS 감사 정책을 생성하는 두 번째 단계입니다. 각 항목은 감사하려는 사용자 또는 그룹을 식별합니다. SACL 항목은 성공한 액세스 시도 또는 실패한 액세스 시도를 감사할지 여부를 정의합니다.

이 작업에 대해

보안 설명자의 SACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 SACL이 포함된 경우 이 명령은 새 ACE를 SACL에 추가합니다. 보안 설명자에 SACL이 포함되어 있지 않으면 명령에서 SACL을 만들고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정의 성공 또는 실패 이벤트에 대해 감사할 권한을 지정하여 SACL 항목을 구성할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)



SACL 항목에 대한 권한을 지정하지 않으면 기본 설정은 "모든 권한"입니다.

"apply to" 매개 변수를 사용하여 상속을 적용하는 방법을 지정하여 SACL 항목을 선택적으로 사용자 지정할 수 있습니다. 이 매개 변수를 지정하지 않으면 기본적으로 이 SACL 항목을 이 폴더, 하위 폴더 및 파일에 적용합니다.

단계

1. 보안 설명자에 SACL 항목을 추가합니다. 'vserver security file-directory NTFS SACL add -vserver vs1 -ntfs -sd sd1 -access-type {failure | success} -account name\_or\_SID optional\_parameters'
- 'vserver security file-directory NTFS SACL add-NTFS-SD SD1-access-type failure-account domain\joe-rights full-control-apply-to this-folder-vs1'
2. SACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS SACL show -vserver vs1 -ntfs -sd sd1 -access-type {failure | success} -account name\_or\_SID'

```
'vserver security file-directory NTFS SACL show -vserver vs1-NTFS-SD SD1-access-type deny-account domain\joe'
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

보안 정책을 생성합니다

SVM(스토리지 가상 머신)에 대한 감사 정책을 생성하는 것은 ACL을 구성하여 파일 또는 폴더에 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각 작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(스토리지 가상 머신)(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

단계

1. 'vserver security file-directory policy create-vserver vserver\_name-policy-name policy\_name' 보안 정책을 생성합니다

```
'vserver security file-directory policy create-policy-name policy1-vserver vs1'
```

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
```

보안 정책에 작업을 추가합니다

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 디렉토리 작업을 통해 적용된 ACL은 SMB 클라이언트 또는 ONTAP CLI를 통해 관리할 수 있습니다.

- 스토리지 레벨 액세스 가드 작업

지정된 볼륨에 Storage-Level Access Guard 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 스토리지 레벨 액세스 가드 작업을 통해 적용된 ACL은 ONTAP CLI를 통해서만 관리할 수 있습니다.

작업에는 파일(또는 폴더) 또는 파일 집합(또는 폴더)의 보안 구성에 대한 정의가 포함됩니다. 정책의 모든 작업은 경로로 고유하게 식별됩니다. 단일 정책 내에서 경로당 하나의 작업만 있을 수 있습니다. 정책에 중복된 작업 항목이 있을 수 없습니다.

정책에 작업 추가 지침:

- 정책당 최대 10,000개의 작업 항목이 있을 수 있습니다.
- 정책에는 하나 이상의 작업이 포함될 수 있습니다.

정책에 둘 이상의 작업이 포함될 수 있지만 파일 디렉터리 및 저장소 수준 액세스 가드 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉터리 작업이 포함되어야 합니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

추가 액세스 권한은 제공하지 않습니다.

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 유형입니다
- 전파 모드
- 인덱스 위치
- 액세스 제어 유형입니다

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉터리 정책 작업 추가 - vserver vserver\_name -policy -name policy\_name -path path -NTFS-SD\_nameoptional\_parameters'

파일 디렉토리는 '-access-control' 파라미터의 기본값입니다. 파일 및 디렉터리 액세스 작업을 구성할 때 액세스 제어 유형을 지정하는 것은 선택 사항입니다.

'vserver security file-directory policy task add-vserver vs1-policy-name policy1-path/home/dir1-security-type NTFS-NTFS-MODE propagate-NTFS-SD SD2-index-num 1-access-control file-directory'를 선택합니다

2. 정책 작업 구성을 확인합니다. 'vserver security file-directory policy task show -vserver vserver\_name -policy -name policy\_name -path path path'

'vserver security file-directory policy task show'를 선택합니다

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor Name					
-----	-----	-----	-----	-----	
-----					
1	/home/dir1	file-directory	ntfs	propagate	sd2

보안 정책을 적용합니다

파일 또는 폴더에 NTFS ACL을 생성하고 적용하는 마지막 단계는 SVM에 감사 정책을 적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.



감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

단계

1. 'vserver security file-directory apply-vserver vserver\_name-policy-name policy\_name' 보안 정책을 적용합니다

```
'vserver security file-directory apply-vserver vs1-policy-name policy1'
```

정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

보안 정책 작업을 모니터링합니다

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 'instance' 매개 변수를 사용해야 합니다.

단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vserver\_name'을 모니터링합니다

'vserver security file-directory job show -vserver vs1'

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

적용된 감사 정책을 확인합니다

감사 정책을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 시스템)의 파일 또는 폴더에 원하는 감사 보안 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

'vserver security file-directory show' 명령을 사용하여 감사 정책 정보를 표시합니다. 표시할 파일 또는 폴더 감사 정책 정보를 가진 데이터의 경로와 데이터가 들어 있는 SVM의 이름을 제공해야 합니다.

단계

1. 감사 정책 설정 표시: 'vserver security file-directory show -vserver\_vserver\_name\_-path\_path\_'

예

다음 명령을 실행하면 SVM VS1 경로의 ""/Corp" 경로에 적용된 감사 정책 정보가 표시됩니다. 경로에 성공 및 성공/실패 SACL 항목이 모두 적용됩니다.



```

cluster::> vserver security file-directory show -vserver vs1 -path /corp

      Vserver: vs1
      File Path: /corp
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

보안 정책 작업을 관리할 때의 고려 사항

특정 상황에서 보안 정책 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을 수정할 수 없습니다. 정책을 수정할 수 있는 조건이나 수정할 수 없는 조건을 이해해야 정책을 수정할 수 있습니다. 정책 수정에는 정책에 할당된 작업을 추가, 제거 또는 수정하고 정책을 삭제 또는 수정하는 작업이 포함됩니다.

해당 정책에 대한 작업이 있고 해당 작업이 다음 상태인 경우 해당 정책에 할당된 보안 정책 또는 작업을 수정할 수 없습니다.

- 작업이 실행 중이거나 진행 중입니다.
- 작업이 일시 중지되었습니다.
- 작업이 재개되고 실행 중 상태입니다.
- 작업이 다른 노드로 장애 조치를 기다리는 경우

다음 상황에서 보안 정책에 대한 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을 성공적으로 수정할 수 있습니다.

- 정책 작업이 중지되었습니다.

- 정책 작업이 성공적으로 완료되었습니다.

#### NTFS 보안 설명자를 관리하는 명령입니다

보안 설명자를 관리하기 위한 특정 ONTAP 명령이 있습니다. 보안 설명자에 대한 정보를 생성, 수정, 삭제 및 표시할 수 있습니다.

원하는 작업	이 명령 사용...
NTFS 보안 설명자를 만듭니다	'vserver security file-directory NTFS create'
기존 NTFS 보안 설명자를 수정합니다	'vserver security file-directory NTFS modify'를 참조하십시오
기존 NTFS 보안 설명자에 대한 정보를 표시합니다	'vserver security file-directory NTFS show'
NTFS 보안 설명자를 삭제합니다	'vserver security file-directory NTFS delete'

자세한 내용은 가상 서버 보안 파일 디렉토리 NTFS 명령에 대한 man 페이지를 참조하십시오.

#### NTFS DACL 액세스 제어 항목을 관리하는 명령입니다

DACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS DACL에 추가할 수 있습니다. DACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS DACL을 관리할 수도 있습니다.

원하는 작업	이 명령 사용...
ACE를 만들어 NTFS DACL에 추가합니다	'vserver security file-directory NTFS DACL add'
NTFS DACL에서 기존 ACE를 수정합니다	'vserver security file-directory NTFS DACL modify'를 선택합니다
NTFS DACL의 기존 ACE에 대한 정보를 표시합니다	'vserver security file-directory NTFS DACL show'
NTFS DACL에서 기존 ACE를 제거합니다	'vserver security file-directory NTFS DACL remove'

자세한 내용은 'vserver security file-directory NTFS DACL' 명령에 대한 man 페이지를 참조하십시오.

#### NTFS SACL 액세스 제어 항목을 관리하는 명령입니다

SACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS SACL에 추가할 수 있습니다. SACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS SACL을 관리할 수도 있습니다.

원하는 작업	이 명령 사용...
ACE를 만들어 NTFS SACL에 추가합니다	'vserver security file-directory NTFS SACL add'
NTFS SACL에서 기존 ACE를 수정합니다	'vserver security file-directory NTFS SACL modify'를 참조하십시오
NTFS SACL의 기존 ACE에 대한 정보를 표시합니다	'vserver security file-directory NTFS SACL show'
NTFS SACL에서 기존 ACE를 제거합니다	'vserver security file-directory NTFS SACL remove'

자세한 내용은 'vserver security file-directory NTFS SACL' 명령에 대한 man 페이지를 참조하십시오.

보안 정책 관리를 위한 명령입니다

보안 정책을 관리하기 위한 특정 ONTAP 명령이 있습니다. 정책에 대한 정보를 표시하고 정책을 삭제할 수 있습니다. 보안 정책을 수정할 수 없습니다.

원하는 작업	이 명령 사용...
보안 정책을 생성합니다	'vserver security file-directory policy create'를 참조하십시오
보안 정책에 대한 정보를 표시합니다	'vserver security file-directory policy show'를 선택합니다
보안 정책을 삭제합니다	'vserver security file-directory policy delete'

자세한 내용은 'vserver security file-directory policy' 명령에 대한 man 페이지를 참조하십시오.

보안 정책 작업을 관리하기 위한 명령입니다

보안 정책 작업에 대한 정보를 추가, 수정, 제거 및 표시하는 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
보안 정책 작업을 추가합니다	'vserver security file-directory policy task add'
보안 정책 작업을 수정합니다	'vserver security file-directory policy task modify'를 선택합니다
보안 정책 작업에 대한 정보를 표시합니다	'vserver security file-directory policy task show'를 선택합니다
보안 정책 작업을 제거합니다	'vserver security file-directory policy task remove'

자세한 내용은 'vserver security file-directory policy task' 명령에 대한 man 페이지를 참조하십시오.

보안 정책 작업 관리를 위한 명령입니다

보안 정책 작업에 대한 정보를 일시 중지, 다시 시작, 중지 및 표시하는 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
보안 정책 작업을 일시 중지합니다	'vserver security file-directory job pause -vserver vserver_name -id integer'
보안 정책 작업을 다시 시작합니다	'vserver security file-directory job resume - vserver vserver_name -id integer'
보안 정책 작업에 대한 정보를 표시합니다	'vserver security file-directory job show -vserver_name' 이 명령을 사용하여 작업의 작업 ID를 확인할 수 있습니다.
보안 정책 작업을 중지합니다	'vserver security file-directory job stop -vserver vserver_name -id integer'

자세한 내용은 'vserver security file-directory job' 명령에 대한 man 페이지를 참조하십시오.

## SMB 공유에 대한 메타데이터 캐시를 구성합니다

### SMB 메타데이터 캐싱의 작동 방식

메타데이터 캐싱을 사용하면 SMB 1.0 클라이언트에서 파일 속성 캐싱을 통해 파일 및 폴더 특성에 더 빠르게 액세스할 수 있습니다. 공유별로 특성 캐싱을 설정하거나 해제할 수 있습니다. 메타데이터 캐시가 설정된 경우 캐시된 항목에 대한 라이브 시간을 구성할 수도 있습니다. 클라이언트가 SMB 2.x 또는 SMB 3.0을 통해 공유에 접속하는 경우에는 메타데이터 캐싱을 구성할 필요가 없습니다.

SMB 메타데이터 캐시가 설정되면 제한된 시간 동안 경로 및 파일 속성 데이터를 저장합니다. 따라서 공통 워크로드를 사용하는 SMB 1.0 클라이언트의 SMB 성능이 향상될 수 있습니다.

특정 작업의 경우 SMB는 경로 및 파일 메타데이터에 대한 여러 개의 동일한 쿼리를 포함할 수 있는 상당한 양의 트래픽을 생성합니다. SMB 메타데이터 캐싱을 사용하여 캐시에서 정보를 가져오는 방식으로 SMB 1.0 클라이언트의 중복 쿼리 수를 줄이고 성능을 향상할 수 있습니다.



가능성은 낮지만 메타데이터 캐시가 오래된 정보를 SMB 1.0 클라이언트에 제공할 수도 있습니다. 귀사의 환경에서 이러한 위험을 감당할 수 없는 경우 이 기능을 활성화하지 마십시오.

### SMB 메타데이터 캐시를 설정합니다

SMB 메타데이터 캐시를 설정하여 SMB 1.0 클라이언트의 SMB 성능을 향상할 수 있습니다. 기본적으로 SMB 메타데이터 캐싱은 해제되어 있습니다.

## 단계

- 원하는 작업을 수행합니다.

원하는 작업	명령 입력...
공유를 생성할 때 SMB 메타데이터 캐싱을 설정합니다	'vserver cifs share create -vserver_vserver_name_ -share-name_share_name_-path_path_-share -properties attributecache'
기존 공유에서 SMB 메타데이터 캐싱을 설정합니다	"vserver cifs 공유 속성 add -vserver_vserver_name_ -share-name_share_name_-share-properties attributecache

## 관련 정보

[SMB 메타데이터 캐시 항목의 수명 구성](#)

[기존 SMB 공유에서 공유 속성 추가 또는 제거](#)

**SMB** 메타데이터 캐시 항목의 수명을 구성합니다

SMB 메타데이터 캐시 항목의 수명을 구성하여 사용자 환경에서 SMB 메타데이터 캐시 성능을 최적화할 수 있습니다. 기본값은 10초입니다.

## 시작하기 전에

SMB 메타데이터 캐시 기능을 활성화해야 합니다. SMB 메타데이터 캐싱이 설정되어 있지 않으면 SMB 캐시 TTL 설정이 사용되지 않습니다.

## 단계

- 원하는 작업을 수행합니다.

다음과 같은 경우 <b>SMB</b> 메타데이터 캐시 항목의 수명을 구성하려는 경우	명령 입력...
공유를 생성합니다	'vserver cifs share-create-vserver_vserver_name_ share-name_share_name_-path_path_-attribute- cache-tl[integer][integerm]'
기존 공유를 수정합니다	'vserver cifs share-modify-vserver_vserver_name_ share-name_share_name_-attribute-cache- tl[integerh][integerm][integer]'

공유를 생성하거나 수정할 때 추가 공유 구성 옵션과 속성을 지정할 수 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

## 파일 잠금 관리

파일 잠금은 사용자가 이전에 다른 사용자가 연 파일에 액세스하지 못하도록 클라이언트 응용 프로그램에서 사용하는 방법입니다. ONTAP가 파일을 잠그는 방법은 클라이언트의 프로토콜에 따라 다릅니다.

클라이언트가 NFS 클라이언트인 경우 잠금이 권고사항이고, 클라이언트가 SMB 클라이언트인 경우 잠금이 필수입니다.

NFS와 SMB 파일 잠금의 차이로 인해 NFS 클라이언트가 SMB 애플리케이션에서 이전에 연 파일에 액세스하지 못할 수 있습니다.

NFS 클라이언트가 SMB 애플리케이션에 의해 잠긴 파일에 액세스하려고 할 때 다음이 발생합니다.

- 혼합 볼륨 또는 NTFS 볼륨에서 rm, rmdir, mv 등의 파일 조작 작업으로 인해 NFS 응용 프로그램이 실패할 수 있습니다.
- NFS 읽기 및 쓰기 작업은 SMB 거부-읽기 및 거부-쓰기 열기 모드에 의해 각각 거부됩니다.
- 배타적 SMB bytelock로 파일의 쓰기 범위가 잠기면 NFS 쓰기 작업이 실패합니다.
- 연결을 끊습니다

- NTFS 파일 시스템의 경우 SMB 및 CIFS 삭제 작업이 지원됩니다.

마지막으로 닫은 후에 파일이 제거됩니다.

- NFS 연결 해제 작업은 지원되지 않습니다.

NTFS 및 SMB 의미가 필요하고 NFS에 대해 마지막 Delete-On-Close 작업이 지원되지 않기 때문에 지원되지 않습니다.

- UNIX 파일 시스템의 경우 연결 해제 작업이 지원됩니다.

NFS 및 UNIX 시맨틱이 필요하기 때문에 지원됩니다.

- 이름 바꾸기

- NTFS 파일 시스템의 경우 SMB 또는 CIFS에서 대상 파일을 열면 대상 파일의 이름을 바꿀 수 있습니다.

- NFS 이름 변경은 지원되지 않습니다.

NTFS 및 SMB 의미가 필요하므로 지원되지 않습니다.

UNIX 보안 스타일 볼륨에서 NFS 링크 해제 및 이름 바꾸기 작업은 SMB 잠금 상태를 무시하고 파일에 대한 액세스를 허용합니다. UNIX 보안 스타일 볼륨에서 다른 모든 NFS 작업은 SMB 잠금 상태를 존중합니다.

## ONTAP에서 읽기 전용 비트를 처리하는 방법

읽기 전용 비트는 파일을 쓰기 가능(사용 안 함)인지 읽기 전용(사용 가능)인지를 나타내기 위해 파일별로 설정됩니다.

Windows를 사용하는 SMB 클라이언트는 파일당 읽기 전용 비트를 설정할 수 있습니다. NFS 클라이언트는 파일당 읽기 전용 비트를 사용하는 프로토콜 작업이 없으므로 파일당 읽기 전용 비트를 설정하지 않습니다.

ONTAP은 Windows를 사용하는 SMB 클라이언트가 해당 파일을 생성할 때 파일에 읽기 전용 비트를 설정할 수 있습니다. 또한 ONTAP은 NFS 클라이언트와 SMB 클라이언트 간에 파일이 공유될 때 읽기 전용 비트를 설정할 수 있습니다. 일부 소프트웨어는 NFS 클라이언트 및 SMB 클라이언트에서 사용할 때 읽기 전용 비트를 사용하도록 설정해야 합니다.

ONTAP가 NFS 클라이언트와 SMB 클라이언트 간에 공유되는 파일에 대해 적절한 읽기 및 쓰기 권한을 유지하려면 다음 규칙에 따라 읽기 전용 비트를 처리합니다.

- NFS는 읽기 전용 비트가 설정된 파일을 쓰기 권한 비트가 설정되지 않은 것처럼 처리합니다.
- NFS 클라이언트가 모든 쓰기 권한 비트를 사용하지 않도록 설정하고 이전에 해당 비트 중 하나 이상이 활성화된 경우 ONTAP은 해당 파일에 대해 읽기 전용 비트를 설정합니다.
- NFS 클라이언트가 쓰기 권한 비트를 설정하면 ONTAP은 해당 파일에 대해 읽기 전용 비트를 해제합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 NFS 클라이언트가 해당 파일에 대한 권한을 검색하려고 하면 파일에 대한 권한 비트가 NFS 클라이언트로 전송되지 않고 ONTAP은 쓰기 권한 비트가 마스킹된 상태로 NFS 클라이언트에 사용 권한 비트를 전송합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 SMB 클라이언트가 읽기 전용 비트를 사용하지 않도록 설정한 경우 ONTAP은 해당 파일에 대한 소유자의 쓰기 권한 비트를 설정합니다.
- 읽기 전용 비트가 설정된 파일은 루트에서만 쓸 수 있습니다.



파일 권한 변경은 SMB 클라이언트에 즉시 적용되지만 NFS 클라이언트가 특성 캐싱을 사용하는 경우 NFS 클라이언트에 즉시 적용되지 않을 수 있습니다.

공유 경로 구성 요소의 잠금 처리에 대한 **ONTAP**과 **Windows**의 차이점

Windows와 달리 ONTAP은 파일이 열려 있는 동안 열려 있는 파일에 대한 경로의 각 구성 요소를 잠그지 않습니다. 이 동작은 SMB 공유 경로에도 영향을 줍니다.

ONTAP은 경로의 각 구성 요소를 잠그지 않으므로 열려 있는 파일 또는 공유 위에 있는 경로 구성 요소의 이름을 바꿀 수 있습니다. 이렇게 하면 특정 응용 프로그램에 문제가 발생하거나 SMB 구성의 공유 경로가 잘못될 수 있습니다. 이로 인해 공유에 액세스할 수 없게 될 수 있습니다.

경로 구성 요소의 이름을 변경하여 발생하는 문제를 방지하려면 사용자나 응용 프로그램이 중요한 디렉터리의 이름을 바꾸지 못하도록 보안 설정을 적용할 수 있습니다.

잠금에 대한 정보를 표시합니다

현재 파일 잠금에 대한 정보를 표시할 수 있습니다. 여기에는 보유한 잠금의 유형 및 잠금 상태, 바이트 범위 잠금에 대한 세부 정보, 공유 잠금 모드, 위임 잠금 및 편의적 잠금, 잠금이 내구성 또는 지속 핸들로 열렸는지 여부 등이 포함됩니다.

이 작업에 대해

NFSv4 또는 NFSv4.1을 통해 설정된 잠금에 대해 클라이언트 IP 주소를 표시할 수 없습니다.

기본적으로 명령은 모든 잠금에 대한 정보를 표시합니다. 명령 매개 변수를 사용하여 특정 SVM(스토리지 가상 머신)의 잠금에 대한 정보를 표시하거나 명령의 출력을 다른 기준으로 필터링할 수 있습니다.

'vserver lock show' 명령은 네 가지 유형의 잠금에 대한 정보를 표시합니다.

- 바이트 범위 잠금 - 파일의 일부만 잠급니다.
- 공유 잠금 - 열린 파일을 잠급니다.
- SMB를 통한 클라이언트 측 캐싱을 제어하는 편의적 잠금 기능
- 위임 - NFSv4.x에서 클라이언트 측 캐싱을 제어합니다

선택적 매개 변수를 지정하면 각 잠금 유형에 대한 중요한 정보를 확인할 수 있습니다. 자세한 내용은 명령에 대한 man 페이지를 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 잠금에 대한 정보를 표시합니다.

예

다음 예에서는 '/vol1/file1' 경로가 있는 파일의 NFSv4 잠금에 대한 요약 정보를 표시합니다. sharelock 액세스 모드는 write-deny\_none 이며, 잠금이 쓰기 위임과 함께 부여되었습니다.

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
vol1    /vol1/file1             lif1         nfsv4     share-level -
                Sharelock Mode: write-deny_none
                delegation -
                Delegation Type: write
```

다음 예에서는 경로 '/data2/data2\_2/intro.pptx'를 사용하여 파일의 SMB 잠금에 대한 자세한 oplock 및 sharelock 정보를 표시합니다. IP 주소가 10.3.1.3인 클라이언트에 write-deny\_none의 공유 잠금 액세스 모드를 가진 파일에 내구성 있는 핸들이 부여됩니다. 배치 oplock 레벨이 있는 리스 oplock이 부여됩니다.

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
```



```

    Bytelock is Superlock: -
        Bytelock is Soft: -
            Oplock Level: -
Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: durable
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

        Vserver: vs1
            Volume: data2_2
Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
        Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
            Lock Protocol: cifs
                Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: -
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

## 잠금 해제

파일 잠금으로 인해 클라이언트가 파일에 액세스하지 못하는 경우 현재 보류된 잠금에 대한 정보를 표시한 다음 특정 잠금을 중단할 수 있습니다. 잠금을 해제해야 하는 시나리오의 예로는 응용 프로그램 디버깅이 있습니다.

이 작업에 대해

'vserver lock break' 명령은 고급 권한 수준 이상에서만 사용할 수 있습니다. 명령에 대한 man 페이지에 자세한 정보가 포함되어 있습니다.

#### 단계

1. 잠금을 해제해야 하는 정보를 찾으려면 'vserver lock show' 명령을 사용합니다.

명령에 대한 man 페이지에 자세한 정보가 포함되어 있습니다.

2. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
3. 다음 작업 중 하나를 수행합니다.

다음을 지정하여 잠금을 해제하려면...	명령 입력...
SVM 이름, 볼륨 이름, LIF 이름 및 파일 경로	'vserver lock break - vserver vserver_name - volume volume_name - path path path -lif lif'
잠금 ID입니다	'vserver lock break-lockid UUID'

4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

## SMB 작업을 모니터링합니다

### SMB 세션 정보를 표시합니다

SMB 연결 및 세션 ID와 세션을 사용하는 워크스테이션의 IP 주소를 포함하여 설정된 SMB 세션에 대한 정보를 표시할 수 있습니다. 세션의 SMB 프로토콜 버전 및 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시하여 세션이 무중단 운영을 지원하는지 여부를 확인할 수 있습니다.

#### 이 작업에 대해

SVM의 모든 세션에 대한 정보를 요약 형식으로 표시할 수 있습니다. 그러나 대부분의 경우 반환되는 출력량이 큼니다. 옵션 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다.

- 옵션 '-fields' 매개 변수를 사용하여 선택한 필드에 대한 출력을 표시할 수 있습니다.

필드를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

- '-instance' 매개 변수를 사용하면 설정된 SMB 세션에 대한 자세한 정보를 표시할 수 있습니다.
- '-fields' 매개 변수 또는 '-instance' 매개 변수를 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
SVM의 모든 세션에 대해 요약 양식을 작성합니다	'vserver cifs session show -vserver vserver_name'을 선택합니다

<b>SMB 세션 정보를 표시하려면...</b>	다음 명령을 입력합니다...
지정된 연결 ID에 있습니다	'vserver cifs session show -vserver vserver_name -connection -id integer'를 선택합니다
지정된 워크스테이션 IP 주소에서	'vserver cifs session show -vserver vserver_name -address workstation_ip_address'
지정된 LIF IP 주소입니다	'vserver cifs session show -vserver vserver_name -lif-address LIF_ip_address'
지정된 노드에서	'vserver cifs session show -vserver vserver_name -node{node_name
local}'	지정된 Windows 사용자로부터
'vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name'	지정된 인증 메커니즘을 사용합니다
'vserver cifs session show -vserver vserver_name -auth-mechanism{NTLMv1	NTLMv2
Kerberos	Anonymous}'
지정된 프로토콜 버전을 사용하여	'vserver cifs session show -vserver vserver_name -protocol -version{SMB1
SMB2	SMB2_1
SMB3	SMB3_1}'을 선택합니다  [NOTE] ==== 지속적으로 사용 가능한 보호 기능과 SMB 멀티 채널은 SMB 3.0 이상 세션에서만 사용할 수 있습니다. 모든 적격 세션에서 해당 상태를 보려면 이 매개 변수를 'MB3' 이상으로 설정한 값으로 지정해야 합니다.  ====
지속적으로 사용 가능한 보호 수준을 지정합니다	'vserver cifs session show -vserver vserver_name -Continuously-available{No

<b>SMB 세션 정보를 표시하려면...</b>	<b>다음 명령을 입력합니다...</b>
Yes	Partial}'  [NOTE] ==== 계속 사용 가능한 상태가 "부분"인 경우 세션에 하나 이상의 열려 있는 연속 사용 가능한 파일이 포함되어 있지만 세션에 계속 사용 가능한 보호 기능이 있는 일부 파일이 열려 있지 않은 것입니다. 'vserver cifs sessions file show' 명령을 사용하여 설정된 세션에서 계속 사용 가능한 보호 기능을 사용하여 열려 있지 않은 파일을 확인할 수 있습니다.  ====
지정된 SMB 서명 세션 상태	'vserver cifs session show -vserver vserver_name -is-session -signed{true

예

다음 명령을 실행하면 IP 주소가 10.1.1.1인 워크스테이션에서 설정된 SVM VS1 세션의 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1        DOMAIN\joe        2         23s
```

다음 명령을 실행하면 SVM VS1 에서 지속적으로 사용 가능한 보호 기능을 지원하는 세션에 대한 자세한 세션 정보가 표시됩니다. 도메인 계정을 사용하여 연결을 만들었습니다.

```
cluster1::> vserver cifs session show -instance -continuously-available  
Yes
```

```
Node: node1  
Vserver: vs1  
Session ID: 1  
Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
Workstation IP address: 10.1.1.2  
Authentication Mechanism: Kerberos  
Windows User: DOMAIN\SERVER1$  
UNIX User: pcuser  
Open Shares: 1  
Open Files: 1  
Open Other: 0  
Connected Time: 10m 43s  
Idle Time: 1m 19s  
Protocol Version: SMB3  
Continuously Available: Yes  
Is Session Signed: false  
User Authenticated as: domain-user  
NetBIOS Name: -  
SMB Encryption Status: Unencrypted
```

다음 명령을 실행하면 SVM VS1 기반 SMB 3.0 및 SMB 멀티 채널을 사용하는 세션에 대한 세션 정보가 표시됩니다. 이 예에서 사용자는 LIF IP 주소를 사용하여 SMB 3.0 지원 클라이언트에서 이 공유에 연결했습니다. 따라서 인증 메커니즘은 NTLMv2로 기본값입니다. 지속적으로 사용 가능한 보호 기능을 사용하여 연결하려면 Kerberos 인증을 사용하여 연결해야 합니다.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```
Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

## 관련 정보

### 열려 있는 SMB 파일에 대한 정보 표시

열려 있는 **SMB** 파일에 대한 정보를 표시합니다

SMB 연결 및 세션 ID, 호스팅 볼륨, 공유 이름 및 공유 경로를 포함하여 열려 있는 SMB 파일에 대한 정보를 표시할 수 있습니다. 파일의 지속적인 사용 가능한 보호 수준에 대한 정보를 표시할 수 있습니다. 이 정보는 열려 있는 파일이 무중단 작업을 지원하는 상태에 있는지 여부를 확인하는 데 유용합니다.

#### 이 작업에 대해

설정된 SMB 세션에서 열린 파일에 대한 정보를 표시할 수 있습니다. 표시된 정보는 SMB 세션 내의 특정 파일에 대한 SMB 세션 정보를 확인해야 할 때 유용합니다.

예를 들어, 열린 파일 중 일부가 지속적으로 사용 가능한 보호 기능을 통해 열려 있고 일부는 지속적으로 사용 가능한 보호 기능을 통해 열려 있지 않은 SMB 세션이 있는 경우(vserver cifs session show 명령의 출력 값이 부분(Partial)인 경우), 이 명령을 사용하여 계속 사용할 수 없는 파일을 확인할 수 있습니다.

선택적 매개 변수 없이 'vserver cifs session file show' 명령을 사용하면 SVM(스토리지 가상 시스템)에서 설정된 SMB 세션의 모든 열려 있는 파일에 대한 정보를 요약 형식으로 표시할 수 있습니다.

그러나 대부분의 경우 반환되는 출력량이 큼니다. 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할

수 있습니다. 이 기능은 열려 있는 파일의 작은 하위 집합에 대한 정보만 보려는 경우에 유용합니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 출력을 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

- '-instance' 매개 변수를 사용하여 열려 있는 SMB 파일에 대한 자세한 정보를 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

열려 있는 <b>SMB</b> 파일을 표시하려면...	다음 명령을 입력합니다...
SVM에 대해 요약 형식으로 표시됩니다	'vserver cifs session file show -vserver vserver_name'을 선택합니다
지정된 노드에서	'vserver cifs session file show -vserver vserver_name -node{node_name
local}'를 선택합니다	지정된 파일 ID에 있습니다
'vserver cifs session file show -vserver vserver_name -file-id integer'를 선택합니다	지정된 SMB 연결 ID에서
'vserver cifs session file show -vserver vserver_name -connection -id integer'를 선택합니다	지정된 SMB 세션 ID에서
'vserver cifs session file show -vserver vserver_name -session-id integer'를 선택합니다	지정된 호스팅 집계에서
'vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name'	지정된 볼륨에서
'vserver cifs session file show -vserver vserver_name -hosting -volume volume volume_name'	지정된 SMB 공유에서
'vserver cifs session file show -vserver vserver_name -share share_name'	지정된 SMB 경로에 있어야 합니다
'vserver cifs session file show -vserver vserver_name -path path path'	지속적으로 사용 가능한 보호 수준을 지정합니다

열려 있는 <b>SMB</b> 파일을 표시하려면...	다음 명령을 입력합니다...
'vserver cifs session file show -vserver vserver_name -Continuously-available{No	Yes}'  [NOTE] ==== 계속 사용 가능한 상태가 '아니요'인 경우 열려 있는 파일은 Takeover와 Giveback에서 중단 없이 복구할 수 없습니다. 또한, 고가용성 관계에 있는 파트너 간의 일반 애그리게이트 재배치에서 복구할 수 없습니다.  ====
지정된 다시 연결된 상태에서	'vserver cifs session file show -vserver vserver_name -re연결됨{No

출력 결과를 구체화하는 데 사용할 수 있는 추가 선택적 매개 변수가 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

예

다음 예에서는 SVM VS1 에서 열린 파일에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1
Node:          node1
Vserver:       vs1
Connection:    3151274158
Session:       1
File           File           Open Hosting           Continuously
ID            Type            Mode Volume           Share           Available
-----
41            Regular        r      data              data            Yes
Path: \mytest.rtf
```

다음 예에서는 SVM VS1에서 파일 ID 82가 있는 개방형 SMB 파일에 대한 자세한 정보를 표시합니다.



```
cluster1::> vsriver cifs session file show -vsriver vs1 -file-id 82
-instance
```

```

Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

#### 관련 정보

[SMB 세션 정보를 표시합니다](#)

사용할 수 있는 통계 개체 및 카운터를 확인합니다

CIFS, SMB, 감사 및 BranchCache 해시 통계에 대한 정보를 얻고 성능을 모니터링하려면 데이터를 가져올 수 있는 개체와 카운터를 알고 있어야 합니다.

#### 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

다음 사항을 확인하고자 하는 경우:	입력...
사용할 수 있는 개체	'통계 카탈로그 개체 쇼'
사용할 수 있는 특정 개체입니다	'통계 카탈로그 객체 객체 객체 객체 객체 객체_이름'을 표시합니다
사용할 수 있는 카운터	'통계 카탈로그 카운터'는 object object_name을 보여준다

사용할 수 있는 개체 및 카운터에 대한 자세한 내용은 man 페이지를 참조하십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 명령을 실행하면 고급 권한 수준에 표시된 대로 클러스터에서 CIFS 및 SMB 액세스와 관련된 선택한 통계 개체에 대한 설명이 표시됩니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                      CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                          The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                  The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                         These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                         These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                        The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

다음 명령을 실행하면 고급 권한 수준에서 표시되는 "CIFS" 개체의 일부 카운터에 대한 정보가 표시됩니다.



이 예제에서는 "CIFS" 객체에 대해 사용 가능한 카운터를 모두 표시하지 않고 출력이 잘립니다.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
-----	-----
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB
...	and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
-----	-----
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

## 통계를 표시합니다

### 통계를 표시합니다

CIFS 및 SMB, 감사 및 BranchCache 해시에 대한 통계를 비롯한 다양한 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

#### 시작하기 전에

객체에 대한 정보를 표시하려면 먼저 '통계 시작' 및 '통계 중지' 명령을 사용하여 데이터 샘플을 수집해야 합니다.

#### 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

에 대한 통계를 표시하려면...	입력...
모든 SMB 버전	'통계 표시 - 객체 CIFS'
SMB 1.0	'스타티틱스 쇼-객체 SMB1'
SMB 2.x 및 SMB 3.0	'스타티틱스 쇼 오브젝트 SMB2'
노드의 CIFS 하위 시스템입니다	'스타티틱스 쇼-객체 nblade_cifs'
멀티프로토콜 감사	'스타티틱스 쇼-객체 감사_ng'
BranchCache 해시 서비스입니다	'스타티틱스 쇼-객체 해시드'
다이나믹 DNS	'통계 표시 - 오브젝트 DDNS_UPDATE'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

#### 관련 정보

[사용할 수 있는 통계 개체 및 카운터 결정](#)

[SMB 서명 세션 통계 모니터링](#)

[BranchCache 통계 표시](#)

[통계를 사용하여 자동 노드 조회 활동을 모니터링합니다](#)

["Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"](#)

["성능 모니터링 설정"](#)

# SMB 클라이언트 기반 서비스 구축

오프라인 파일을 사용하여 오프라인 사용을 위해 파일 캐싱을 허용합니다

오프라인 파일을 사용하여 오프라인 사용을 위한 파일 캐싱 개요

ONTAP는 오프라인 사용을 위해 파일을 로컬 호스트에 캐시할 수 있는 Microsoft 오프라인 파일 기능 또는 \_클라이언트측 캐싱\_을 지원합니다. 사용자는 오프라인 파일 기능을 사용하여 네트워크에서 연결이 끊어진 경우에도 파일 작업을 계속할 수 있습니다.

Windows 사용자 문서 및 프로그램이 자동으로 공유에서 캐시되는지 아니면 파일을 수동으로 캐시하도록 선택해야 하는지 여부를 지정할 수 있습니다. 수동 캐싱은 새 공유에 대해 기본적으로 설정됩니다. 오프라인으로 사용할 수 있는 파일은 Windows 클라이언트의 로컬 디스크와 동기화됩니다. 동기화는 특정 스토리지 시스템 공유에 대한 네트워크 접속이 복구되는 경우에 발생합니다.

오프라인 파일 및 폴더는 CIFS 서버에 저장된 파일 및 폴더의 버전과 동일한 액세스 권한을 유지하므로 오프라인 파일 및 폴더에 대한 작업을 수행하려면 CIFS 서버에 저장된 파일 및 폴더에 대한 충분한 권한이 있어야 합니다.

사용자 및 네트워크의 다른 사용자가 동일한 파일을 변경한 경우 사용자는 파일의 로컬 버전을 네트워크에 저장하거나 다른 버전을 유지하거나 둘 다 저장할 수 있습니다. 사용자가 두 버전을 모두 유지할 경우 로컬 사용자의 변경 내용이 있는 새 파일이 로컬에 저장되고 캐시된 파일은 CIFS 서버에 저장된 파일 버전의 변경 내용으로 덮어쓰입니다.

공유 구성 설정을 사용하여 공유 단위로 오프라인 파일을 구성할 수 있습니다. 공유를 만들거나 수정할 때 네 개의 오프라인 폴더 구성 중 하나를 선택할 수 있습니다.

- 캐싱이 없습니다

공유에 대한 클라이언트 측 캐싱을 해제합니다. 파일과 폴더는 클라이언트에 로컬로 자동으로 캐시되지 않으며 사용자는 파일 또는 폴더를 로컬로 캐시하도록 선택할 수 없습니다.

- 수동 캐싱

공유에 캐시할 파일을 수동으로 선택할 수 있습니다. 기본 설정입니다. 기본적으로 파일 또는 폴더는 로컬 클라이언트에 캐시되지 않습니다. 사용자는 오프라인 사용을 위해 로컬로 캐시할 파일과 폴더를 선택할 수 있습니다.

- 자동 문서 캐싱

사용자 문서를 공유에 자동으로 캐시할 수 있습니다. 액세스한 파일 및 폴더만 로컬로 캐시됩니다.

- 자동 프로그램 캐싱

프로그램 및 사용자 문서를 자동으로 공유에 캐시할 수 있습니다. 액세스한 파일, 폴더 및 프로그램만 로컬로 캐시됩니다. 또한 이 설정을 사용하면 클라이언트가 네트워크에 연결되어 있는 경우에도 로컬로 캐시된 실행 파일을 실행할 수 있습니다.

Windows 서버 및 클라이언트에서 오프라인 파일을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

[로밍 프로필을 사용하여 SVM과 연결된 CIFS 서버에 사용자 프로필을 중앙에서 저장합니다](#)

폴더 리디렉션을 사용하여 CIFS 서버에 데이터를 저장합니다

BranchCache를 사용하여 지사에 SMB 공유 콘텐츠를 캐싱합니다

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

오프라인 파일 사용에 대한 요구 사항

CIFS 서버에서 Microsoft 오프라인 파일 기능을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

**ONTAP** 버전 요구 사항

ONTAP 릴리스는 오프라인 파일을 지원합니다.

**SMB** 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 오프라인 파일을 지원합니다.

**Windows** 클라이언트 요구 사항

Windows 클라이언트는 오프라인 파일을 지원해야 합니다.

오프라인 파일 기능을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"[mysupport.netapp.com/matrix](http://mysupport.netapp.com/matrix)"

오프라인 파일 배포 지침

홈 디렉토리에 'showsnapshot' 공유 속성이 설정된 홈 디렉토리 공유에 오프라인 파일을 배포할 때 이해해야 하는 몇 가지 중요한 지침이 있습니다.

오프라인 파일이 구성된 홈 디렉토리 공유에 'showsnapshot' 공유 속성이 설정되어 있으면 Windows 클라이언트는 사용자의 홈 디렉토리에 있는 '~snapshot' 폴더 아래에 있는 모든 스냅샷 복사본을 캐시합니다.

다음 중 하나가 참인 경우 Windows 클라이언트는 홈 디렉토리 아래에 있는 모든 스냅샷 복사본을 캐시합니다.

- 사용자가 클라이언트에서 홈 디렉토리를 오프라인으로 사용할 수 있도록 합니다.

홈 디렉토리에 있는 '~snapshot' 폴더의 내용이 포함되어 오프라인으로 사용할 수 있습니다.

- 사용자는 '내 문서'와 같은 폴더를 CIFS 서버 공유에 있는 홈 디렉토리의 루트로 리디렉션하도록 폴더 리디렉션을 구성합니다.

일부 Windows 클라이언트는 리디렉션된 폴더를 자동으로 오프라인으로 사용할 수 있도록 만들 수 있습니다. 폴더가 홈 디렉토리의 루트로 리디렉션되면 "~snapshot" 폴더가 캐시된 오프라인 콘텐츠에 포함됩니다.



"~snapshot" 폴더가 오프라인 파일에 포함된 오프라인 파일 배포를 피해야 합니다. "~snapshot" 폴더의 스냅샷 복사본에는 ONTAP이 스냅샷 복사본을 생성한 시점의 볼륨에 있는 모든 데이터가 포함됩니다. 따라서 "~snapshot" 폴더의 오프라인 복사본을 만들면 클라이언트에서 상당한 로컬 스토리지가 사용되며 오프라인 파일 동기화 중에 네트워크 대역폭이 소모되고 오프라인 파일을 동기화하는 데 걸리는 시간이 늘어납니다.

CLI를 사용하여 **SMB** 공유에서 오프라인 파일 지원을 구성합니다

SMB 공유를 생성할 때 또는 언제든지 기존 SMB 공유를 수정하여 오프라인 파일 4개 설정 중 하나를 지정하여 ONTAP CLI를 사용하여 오프라인 파일 지원을 구성할 수 있습니다. 수동 오프라인 파일 지원은 기본 설정입니다.

이 작업에 대해

오프라인 파일 지원을 구성할 때 다음 네 가지 오프라인 파일 설정 중 하나를 선택할 수 있습니다.

설정	설명
"없음"	Windows 클라이언트가 이 공유의 모든 파일을 캐싱하지 않습니다.
수동	Windows 클라이언트의 사용자가 캐시할 파일을 수동으로 선택할 수 있습니다.
문서	Windows 클라이언트가 오프라인 액세스를 위해 사용자가 사용하는 사용자 문서를 캐시할 수 있도록 합니다.
프로그램	Windows 클라이언트가 오프라인 액세스를 위해 사용자가 사용하는 프로그램을 캐시에 저장하도록 허용합니다. 클라이언트는 공유를 사용할 수 있는 경우에도 오프라인 모드에서 캐시된 프로그램 파일을 사용할 수 있습니다.

오프라인 파일 설정은 하나만 선택할 수 있습니다. 기존 SMB 공유에서 오프라인 파일 설정을 수정하면 새 오프라인 파일 설정이 원래 설정으로 대체됩니다. 기존의 다른 SMB 공유 구성 설정 및 공유 속성은 제거 또는 교체되지 않습니다. 이러한 구성 작업은 명시적으로 제거 또는 변경될 때까지 유효합니다.

단계

1. 적절한 작업을 수행합니다.

에서 오프라인 파일을 구성하려면...	명령 입력...
새로운 SMB 공유	'vserver cifs share create - vservice vservice_name -share-name share_name -path path -offline -files{none
manual	documents
programs}'	기존 SMB 공유입니다

에서 오프라인 파일을 구성하려면...	명령 입력...
'vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files{none	manual
documents	programs}'

2. SMB 공유 구성이 올바른지 확인합니다. 'vserver cifs share show -vserver vserver\_name -share-name share\_name -instance'

예

다음 명령을 실행하면 오프라인 파일이 "문서"로 설정된 "data1"이라는 SMB 공유가 생성됩니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: Offline files
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: documents
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

다음 명령을 실행하면 오프라인 파일 설정을 '수동'으로 변경하고 파일 및 디렉토리 모드 생성 마스크에 대한 값을 추가하여 "data1"이라는 기존 SMB 공유가 수정됩니다.



```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
    CIFS Server NetBIOS Name: VS1
                Path: /data1
    Share Properties: oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: 644
    Directory Mode Creation Mask: 777
    Share Comment: Offline files
    Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
    Volume Name: -
    Offline Files: manual
    Vscan File-Operations Profile: standard
    Maximum Tree Connections on Share: 4294967295
    UNIX Group for File Create: -
```

## 관련 정보

### 기존 SMB 공유에서 공유 속성 추가 또는 제거

컴퓨터 관리 **MMC**를 사용하여 **SMB** 공유에서 오프라인 파일 지원을 구성합니다

사용자가 오프라인에서 사용할 수 있도록 로컬로 파일을 캐시하도록 허용하려면 컴퓨터 관리 MMC(Microsoft Management Console)를 사용하여 오프라인 파일 지원을 구성할 수 있습니다.

#### 단계

1. Windows 서버에서 MMC를 열려면 Windows 탐색기에서 로컬 컴퓨터 아이콘을 마우스 오른쪽 단추로 클릭한 다음 \* 관리 \* 를 선택합니다.
2. 왼쪽 패널에서 \* 컴퓨터 관리 \* 를 선택합니다.
3. 작업 \* > \* 다른 컴퓨터에 연결 \* 을 선택합니다.

컴퓨터 선택 대화 상자가 나타납니다.

4. CIFS 서버의 이름을 입력하거나 \* Browse \* 를 클릭하여 CIFS 서버를 찾습니다.

CIFS 서버의 이름이 SVM(Storage Virtual Machine) 호스트 이름과 같으면 SVM 이름을 입력합니다. CIFS 서버 이름이 SVM 호스트 이름과 다른 경우 CIFS 서버의 이름을 입력합니다.

5. 확인 \* 을 클릭합니다.
6. 콘솔 트리에서 \* 시스템 도구 \* > \* 공유 폴더 \* 를 클릭합니다.
7. 공유 \* 를 클릭합니다.
8. 결과 창에서 공유를 마우스 오른쪽 버튼으로 클릭합니다.
9. 속성 \* 을 클릭합니다.

선택한 공유의 속성이 표시됩니다.

10. 일반 \* 탭에서 \* 오프라인 설정 \* 을 클릭합니다.

오프라인 설정 대화 상자가 나타납니다.

11. 필요에 따라 오프라인 사용 가능성 옵션을 구성합니다.
12. 확인 \* 을 클릭합니다.

로밍 프로필을 사용하여 **SVM**과 연결된 **SMB** 서버에 사용자 프로필을 중앙에서 저장합니다

로밍 프로필을 사용하여 **SVM** 개요와 관련된 **SMB** 서버에 사용자 프로필을 중앙에서 저장합니다

ONTAP는 SVM(스토리지 가상 머신)과 연결된 CIFS 서버에 Windows 로밍 프로필을 저장할 수 있도록 지원합니다. 사용자 로밍 프로파일을 구성하면 사용자가 로그인하는 위치에 관계없이 자동 리소스 사용 가능 여부 등의 이점이 제공됩니다. 또한 로밍 프로필은 사용자 프로필의 관리 및 관리를 간소화합니다.

로밍 사용자 프로필에는 다음과 같은 이점이 있습니다.

- 자동 리소스 가용성

사용자가 Windows 8, Windows 7, Windows 2000 또는 Windows XP를 실행하는 네트워크의 컴퓨터에 로그인하면 사용자의 고유한 프로필을 자동으로 사용할 수 있습니다. 사용자는 네트워크에서 사용하는 각 컴퓨터에 프로파일을 만들 필요가 없습니다.

- 간편한 컴퓨터 교체

사용자 프로필 정보는 모두 네트워크에서 별도로 유지되므로 사용자의 프로필을 새 대체 컴퓨터에 쉽게 다운로드할 수 있습니다. 사용자가 새 컴퓨터에 처음 로그인하면 사용자 프로필의 서버 복사본이 새 컴퓨터에 복사됩니다.

관련 정보

[오프라인 파일을 사용하여 오프라인 사용을 위해 파일 캐싱을 허용합니다](#)

[폴더 리디렉션을 사용하여 CIFS 서버에 데이터를 저장합니다](#)

로밍 프로필 사용에 대한 요구 사항

CIFS 서버에서 Microsoft의 로밍 프로필을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

## ONTAP 버전 요구 사항

ONTAP는 로밍 프로필을 지원합니다.

## SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 로밍 프로필을 지원합니다.

## Windows 클라이언트 요구 사항

사용자가 로밍 프로필을 사용하려면 Windows 클라이언트가 이 기능을 지원해야 합니다.

로밍 프로필을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

## "NetApp 상호 운용성 매트릭스 툴"

로밍 프로필을 구성합니다

사용자가 네트워크의 컴퓨터에 로그인할 때 자동으로 사용자 프로필을 사용할 수 있도록 하려면 Active Directory 사용자 및 컴퓨터 MMC 스냅인을 통해 로밍 프로필을 구성할 수 있습니다. Windows Server에서 로밍 프로필을 구성하는 경우 Active Directory 관리 센터를 사용할 수 있습니다.

단계

1. Windows 서버에서 Active Directory 사용자 및 컴퓨터 MMC(또는 Windows 서버의 Active Directory 관리 센터)를 엽니다.
2. 로밍 프로필을 구성할 사용자를 찾습니다.
3. 사용자를 마우스 오른쪽 단추로 클릭하고 \* 속성 \* 을 클릭합니다.
4. 프로필 \* 탭에서 사용자의 로밍 프로필을 저장할 공유의 프로파일 경로를 입력한 다음 '%username%'을(를) 입력합니다.

예를 들어, 프로파일 경로는 다음과 같습니다: '\\vs1.example.com\profiles\%username%'. 사용자가 처음 로그인하면 '%username%'이(가) 사용자 이름으로 대체됩니다.



'\\vs1.example.com\profiles\%username%' 경로에서 'profiles'는 SVM(Storage Virtual Machine) VS1 공유에 대한 공유 이름이며 모든 사람에게 모든 권한이 부여됩니다.

5. 확인 \* 을 클릭합니다.

## SMB 서버에 데이터를 저장하려면 폴더 리디렉션을 사용합니다

폴더 리디렉션을 사용하여 **SMB** 서버에 데이터 저장 개요

ONTAP는 사용자 또는 관리자가 로컬 폴더의 경로를 CIFS 서버의 위치로 리디렉션할 수 있도록 Microsoft 폴더 리디렉션을 지원합니다. SMB 공유에 데이터가 저장되어 있더라도 리디렉션된 폴더가 로컬 Windows 클라이언트에 저장된 것처럼 나타납니다.

폴더 리디렉션은 주로 홈 디렉터리를 이미 배포했으며 기존 홈 디렉터리 환경과의 호환성을 유지하고자 하는 조직을

위한 것입니다.

- 문서, 바탕 화면, 시작 메뉴 등을 리디렉션할 수 있는 폴더의 예로 들 수 있습니다.
- 사용자는 Windows 클라이언트에서 폴더를 리디렉션할 수 있습니다.
- 관리자는 Active Directory에서 GPO를 구성하여 폴더 리디렉션을 중앙 집중식으로 구성 및 관리할 수 있습니다.
- 관리자가 로밍 프로필을 구성한 경우 폴더 리디렉션을 통해 관리자가 사용자 데이터를 프로필 데이터에서 나눌 수 있습니다.
- 관리자는 폴더 리디렉션 및 오프라인 파일을 함께 사용하여 로컬 폴더의 데이터 스토리지를 CIFS 서버로 리디렉션하는 동시에 사용자가 콘텐츠를 로컬로 캐시할 수 있습니다.

#### 관련 정보

[오프라인 파일을 사용하여 오프라인 사용을 위해 파일 캐싱을 허용합니다](#)

[로밍 프로필을 사용하여 SVM과 연결된 CIFS 서버에 사용자 프로필을 중앙에서 저장합니다](#)

#### 폴더 리디렉션 사용 요구 사항

CIFS 서버에서 Microsoft의 폴더 리디렉션을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

##### ONTAP 버전 요구 사항

ONTAP는 Microsoft 폴더 리디렉션을 지원합니다.

##### SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP는 모든 버전의 SMB에서 Microsoft의 폴더 리디렉션을 지원합니다.

##### Windows 클라이언트 요구 사항

사용자가 Microsoft의 폴더 리디렉션을 사용하려면 Windows 클라이언트가 이 기능을 지원해야 합니다.

폴더 리디렉션을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

#### 폴더 리디렉션을 구성합니다

Windows 속성 창을 사용하여 폴더 리디렉션을 구성할 수 있습니다. 이 방법을 사용하면 Windows 사용자가 SVM 관리자의 도움 없이 폴더 리디렉션을 구성할 수 있다는 이점이 있습니다.

#### 단계

1. Windows 탐색기에서 네트워크 공유로 리디렉션할 폴더를 마우스 오른쪽 단추로 클릭합니다.
2. 속성 \* 을 클릭합니다.

선택한 공유의 속성이 표시됩니다.

3. 바로 가기 \* 탭에서 \* 대상 \* 을 클릭하고 선택한 폴더를 리디렉션할 네트워크 위치의 경로를 지정합니다.

예를 들어, 폴더를 "Q:\\"에 매핑된 홈 디렉토리의 "ata" 폴더로 리디렉션하려면 "Q:\data"를 대상으로 지정합니다.

4. 확인 \* 을 클릭합니다.

오프라인 폴더 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

#### 관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

### SMB 2.x를 사용하여 Windows 클라이언트에서 ~snapshot 디렉토리에 액세스합니다

SMB 2.x를 사용하는 Windows 클라이언트의 '~snapshot' 디렉토리에 액세스하는 방법은 SMB 1.0에 사용되는 방법과 다릅니다. SMB 2.x 연결을 사용할 때 Snapshot 복사본에 저장된 데이터에 성공적으로 액세스하기 위해 '~snapshot' 디렉토리에 액세스하는 방법을 이해해야 합니다.

SVM 관리자는 가상 서버 CIFS 공유 속성 제품군의 명령을 사용하여 'showsnapshot' 공유 속성을 활성화하거나 비활성화하여 Windows 클라이언트의 사용자가 공유의 '~snapshot' 디렉토리를 보고 액세스할 수 있는지 여부를 제어합니다.

'showsnapshot' 공유 속성을 비활성화하면 SMB 2.x를 사용하는 Windows 클라이언트의 사용자는 '~snapshot' 디렉토리를 볼 수 없으며 '~snapshot' 디렉토리의 경로를 수동으로 입력하거나 디렉토리 내의 특정 Snapshot 복제본에 액세스할 수 없습니다.

'showsnapshot' 공유 속성이 활성화되면 SMB 2.x를 사용하는 Windows 클라이언트의 사용자는 공유 루트 또는 공유 루트 아래의 연결 지점 또는 디렉토리 내에서 '~snapshot' 디렉토리를 볼 수 없습니다. 그러나 공유에 접속한 후에는 공유 경로의 끝에 수동으로 \~snapshot을 추가하여 숨겨진 '~snapshot' 디렉토리에 액세스할 수 있습니다. 숨겨진 '~snapshot' 디렉토리는 두 개의 진입점에서 액세스할 수 있습니다.

- 공유 루트에 있습니다
- 공유 공간의 모든 접합 지점에서

공유 내의 비접속 하위 디렉토리에서는 숨겨진 '~snapshot' 디렉토리에 액세스할 수 없습니다.

#### 예

다음 예제에서 보여 주는 구성을 사용하면 "eng" 공유에 SMB 2.x가 연결되어 있는 Windows 클라이언트의 사용자가 공유 경로 및 경로의 모든 연결 지점에서 공유 경로에 "\~snapshot"을 수동으로 추가하여 '~snapshot' 디렉토리에 액세스할 수 있습니다. 숨겨진 '~snapshot' 디렉토리는 다음 세 가지 경로에서 액세스할 수 있습니다.

- '\\VS1\ENG\~스냅샷'
- '\\VS1\ENG\projects1\~스냅샷'
- '\\VS1\ENG\projects2\~스냅샷'

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root        /
vs1      vs1_vol1        /eng
vs1      vs1_vol2        /eng/projects1
vs1      vs1_vol3        /eng/projects2

cluster1::> vsserver cifs share show
Vserver  Share  Path  Properties  Comment  ACL
-----
vs1      eng    /eng  oplocks     -        Everyone / Full Control
        changenotify
        browsable
        showsnapshot
```

## 이전 버전을 사용하여 파일 및 폴더를 복구합니다

이전 버전 개요를 사용하여 파일 및 폴더를 복구합니다

Microsoft 이전 버전을 사용하는 기능은 Snapshot 복사본을 일부 형식으로 지원하고 사용하도록 설정한 파일 시스템에 적용할 수 있습니다. 스냅샷 기술은 ONTAP의 핵심 요소입니다. 사용자는 Microsoft 이전 버전 기능을 사용하여 Windows 클라이언트에서 Snapshot 복사본의 파일과 폴더를 복구할 수 있습니다.

이전 버전 기능을 사용하면 사용자는 스토리지 관리자의 개입 없이 스냅샷 복사본을 탐색하거나 스냅샷 복사본에서 데이터를 복원할 수 있습니다. 이전 버전은 구성할 수 없습니다. 항상 활성화되어 있습니다. 스토리지 관리자가 공유에 스냅샷 복사본을 사용하도록 설정한 경우 이전 버전을 사용하여 다음 작업을 수행할 수 있습니다.

- 실수로 삭제된 파일을 복구합니다.
- 실수로 파일을 덮어쓴 경우 복구
- 작업 중 파일 버전을 비교합니다.

스냅샷 복사본에 저장된 데이터는 읽기 전용입니다. 파일을 변경하려면 파일 복사본을 다른 위치에 저장해야 합니다. 스냅샷 복사본은 주기적으로 삭제되므로 이전 버전의 파일을 무기한 보존하려는 경우 이전 버전에 포함된 파일 복사본을 만들어야 합니다.

### Microsoft 이전 버전 사용에 대한 요구 사항

CIFS 서버에서 이전 버전을 사용하려면 먼저 ONTAP 및 SMB의 버전과 지원 대상 Windows 클라이언트를 알아야 합니다. 스냅샷 복사본 설정 요구사항에 대해서도 알아야 합니다.

### ONTAP 버전 요구 사항

이전 버전을 지원합니다.

## SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 이전 버전을 지원합니다.

## Windows 클라이언트 요구 사항

사용자가 이전 버전을 사용하여 스냅샷 복사본의 데이터에 액세스할 수 있으려면 먼저 Windows 클라이언트가 이 기능을 지원해야 합니다.

이전 버전을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

## "NetApp 상호 운용성 매트릭스 툴"

### 스냅샷 복사본 설정에 대한 요구사항

이전 버전을 사용하여 스냅샷 복사본의 데이터에 액세스하려면 활성화된 스냅샷 정책이 데이터가 포함된 볼륨에 연결되어 있어야 하고, 클라이언트가 스냅샷 데이터에 액세스할 수 있어야 하며, 스냅샷 복사본이 존재해야 합니다.

이전 버전 탭을 사용하여 스냅샷 복사본 데이터를 보고 관리할 수 있습니다

Windows 클라이언트 시스템의 사용자는 Windows 속성 창의 이전 버전 탭을 사용하여 SVM(스토리지 가상 머신) 관리자를 참여시키지 않고도 스냅샷 복사본에 저장되어 있는 데이터를 복원할 수 있습니다.

### 이 작업에 대해

관리자가 공유가 포함된 볼륨에서 스냅샷 복사본을 사용하도록 설정하고 관리자가 스냅샷 복사본을 표시하도록 공유를 구성한 경우, 이전 버전 탭을 사용하여 SVM에 저장된 데이터의 스냅샷 복사본에 있는 데이터를 보고 관리할 수 있습니다.

### 단계

1. Windows 탐색기에서 CIFS 서버에 저장된 데이터의 매핑된 드라이브 콘텐츠를 표시합니다.
2. 스냅샷 복사본을 보거나 관리할 매핑된 네트워크 드라이브에서 파일 또는 폴더를 마우스 오른쪽 단추로 클릭합니다.
3. 속성 \* 을 클릭합니다.

선택한 파일 또는 폴더의 속성이 표시됩니다.

4. 이전 버전 \* 탭을 클릭합니다.

선택한 파일 또는 폴더의 사용 가능한 스냅샷 복사본 목록이 폴더 버전: 상자에 표시됩니다. 나열된 스냅샷 복사본은 스냅샷 복사본 이름 접두사 및 생성 타임 스탬프로 식별됩니다.

5. 폴더 버전: \* 상자에서 관리할 파일 또는 폴더의 복사본을 마우스 오른쪽 단추로 클릭합니다.
6. 적절한 작업을 수행합니다.

원하는 작업	다음을 수행합니다.
해당 스냅샷 복사본의 데이터를 봅니다	열기 * 를 클릭합니다.
해당 스냅샷 복사본에서 데이터 복사본을 생성합니다	복사 * 를 클릭합니다.

스냅샷 복사본의 데이터는 읽기 전용입니다. 이전 버전 탭에 나열된 파일과 폴더를 수정하려면 쓰기 가능한 위치에 수정할 파일 및 폴더의 복사본을 저장하고 복사본을 수정해야 합니다.

7. 스냅샷 데이터 관리를 마친 후 \* OK \* 를 클릭하여 \* Properties \* 대화 상자를 닫습니다.

이전 버전 탭을 사용하여 스냅샷 데이터를 보고 관리하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

#### 관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

이전 버전에서 사용할 수 있는 스냅샷 복사본이 있는지 확인합니다

활성화된 스냅샷 정책이 공유가 포함된 볼륨에 적용되고 볼륨 구성에서 스냅샷 복사본에 액세스할 수 있는 경우에만 이전 버전 탭에서 스냅샷 복사본을 볼 수 있습니다. 이전 버전 액세스 권한을 가진 사용자를 지원할 때 스냅샷 복사본의 가용성을 확인하는 것이 좋습니다.

#### 단계

1. 공유 데이터가 상주하는 볼륨에 자동 스냅샷 복사본이 활성화되어 있는지 여부와 클라이언트가 스냅샷 디렉토리에 액세스할 수 있는지 여부를 확인합니다. 'volume show -vserver -name -volume volume -name -vserver 필드, 볼륨, snapdir -access, snapshot-policy, snapshot-count'

출력에는 볼륨과 연관된 스냅샷 정책, 클라이언트 스냅샷 디렉토리 액세스 설정 여부 및 사용 가능한 스냅샷 복사본 수가 표시됩니다.

2. 연결된 스냅샷 정책이 'volume snapshot policy show-policy policy-name'으로 설정되어 있는지 확인합니다
3. 사용 가능한 스냅샷 복사본 'volume snapshot show-volume volume\_name'을 나열합니다

스냅샷 정책 및 스냅샷 일정 구성 및 관리에 대한 자세한 내용은 을 참조하십시오 "데이터 보호".

#### 예

다음 예에서는 공유 데이터 및 "data1"의 사용 가능한 스냅샷 복사본이 포함된 "data1"이라는 볼륨과 연결된 스냅샷 정책에 대한 정보를 표시합니다.



```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

                Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule      Count      Prefix      SnapMirror Label
    -----
    hourly        6      hourly      -
    daily          2      daily       daily
    weekly         2      weekly      weekly

cluster1::> volume snapshot show -volume data1

                ---Blocks---
Vserver  Volume  Snapshot                State      Size  Total%  Used%
-----
vs1      data1
        weekly.2012-12-16_0015  valid      408KB    0%    1%
        daily.2012-12-22_0010  valid      420KB    0%    1%
        daily.2012-12-23_0010  valid      192KB    0%    0%
        weekly.2012-12-23_0015  valid      360KB    0%    1%
        hourly.2012-12-23_1405  valid      196KB    0%    0%
        hourly.2012-12-23_1505  valid      196KB    0%    0%
        hourly.2012-12-23_1605  valid      212KB    0%    0%
        hourly.2012-12-23_1705  valid      136KB    0%    0%
        hourly.2012-12-23_1805  valid      200KB    0%    0%
        hourly.2012-12-23_1905  valid      184KB    0%    0%
```

## 관련 정보

[이전 버전 액세스를 사용하도록 스냅샷 구성을 생성합니다](#)

## "데이터 보호"

[이전 버전 액세스를 사용하도록 스냅샷 구성을 생성합니다](#)

스냅샷 복사본에 대한 클라이언트 액세스가 설정되어 있고 스냅샷 복사본이 있다면 이전 버전 기능은 항상 사용할 수 있습니다. 스냅샷 복사본 구성이 이러한 요구사항을 충족하지 않으면 이를 위한 스냅샷 복사본 구성을 생성할 수 있습니다.

## 단계

1. 이전 버전 액세스를 허용할 공유가 포함된 볼륨에 연결된 스냅샷 정책이 없는 경우 스냅샷 정책을 볼륨에 연결하고 '볼륨 수정' 명령을 사용하여 활성화합니다.

볼륨 수정 명령에 대한 자세한 내용은 man 페이지를 참조하십시오.

2. "volume modify" 명령을 사용하여 스냅샷 복사본에 대한 액세스를 설정하고 "-snap-dir" 옵션을 "true"로 설정합니다.

볼륨 수정 명령에 대한 자세한 내용은 man 페이지를 참조하십시오.

3. "volume show" 및 "volume snapshot policy show" 명령을 사용하여 스냅샷 정책이 활성화되어 있고 스냅샷 디렉토리에 대한 액세스가 활성화되어 있는지 확인합니다.

'volume show' 및 'volume snapshot policy show' 명령 사용에 대한 자세한 내용은 man 페이지를 참조하십시오.

스냅샷 정책 및 스냅샷 일정 구성 및 관리에 대한 자세한 내용은 을 참조하십시오 ["데이터 보호"](#).

## 관련 정보

["데이터 보호"](#)

## 교차점이 포함된 디렉토리 복원 지침

이전 버전을 사용하여 교차점이 포함된 폴더를 복원할 때 유의해야 할 몇 가지 지침이 있습니다.

이전 버전을 사용하여 정션 포인트인 하위 폴더가 있는 폴더를 복원할 때 "액세스 거부" 오류로 인해 복구가 실패할 수 있습니다.

복원하려는 폴더에 '-parent' 옵션과 함께 'vol show' 명령을 사용하여 교차점이 있는지 여부를 확인할 수 있습니다. 또한 'vserver security trace' 명령을 사용하여 파일 및 폴더 액세스 문제에 대한 자세한 로그를 생성할 수 있습니다.

## 관련 정보

[NAS 네임스페이스에서 데이터 볼륨 생성 및 관리](#)

# SMB 서버 기반 서비스 구축

## 홈 디렉토리를 관리합니다

### ONTAP에서 동적 홈 디렉토리를 활성화하는 방법

ONTAP 홈 디렉토리를 사용하면 연결된 사용자와 변수 집합을 기반으로 서로 다른 디렉토리에 매핑되는 SMB 공유를 구성할 수 있습니다. 각 사용자에게 대해 별도의 공유를 생성하는 대신 몇 가지 홈 디렉토리 매개 변수를 사용하여 하나의 공유를 구성하여 진입점(공유)과 홈 디렉토리(SVM의 디렉토리) 간의 사용자 관계를 정의할 수 있습니다.

게스트 사용자로 로그인한 사용자는 홈 디렉토리가 없으며 다른 사용자의 홈 디렉토리에 액세스할 수 없습니다. 사용자가 디렉토리에 매핑되는 방식을 결정하는 변수는 네 가지입니다.

- \* 공유 이름 \*

사용자가 연결하는 공유의 이름입니다. 이 공유에 대한 홈 디렉토리 속성을 설정해야 합니다.

공유 이름에는 다음 동적 이름을 사용할 수 있습니다.

- '%w'(사용자의 Windows 사용자 이름)
- '%d'(사용자의 Windows 도메인 이름)
- '%u'(사용자가 매핑한 UNIX 사용자 이름)공유 이름을 모든 홈 디렉토리에 고유하도록 하려면 공유 이름에 '%w' 또는 '%u' 변수가 포함되어야 합니다. 공유 이름에는 "%d"와 "%w" 변수(예: "%d"/"%w")가 모두 포함될 수 있으며, 공유 이름에는 정적 부분과 변수 부분(예: home\_""%w")이 포함될 수 있습니다.

• \* 공유 경로 \*

이 경로는 공유에 의해 정의되고 공유 이름 중 하나와 연관되며, SVM의 루트에서 사용자의 전체 홈 디렉토리 경로를 생성하기 위해 각 검색 경로에 추가됩니다. 정적(예: "home"), 동적(예: "%w") 또는 두 가지 조합(예: "eng/%w")일 수 있습니다.

• \* 검색 경로 \*

ONTAP에서 홈 디렉토리를 검색하도록 지정하는 SVM 루트의 절대 경로 세트입니다. 'vserver cifs home-directory search-path add' 명령을 사용하여 하나 이상의 검색 경로를 지정할 수 있습니다. 여러 개의 검색 경로를 지정하면 ONTAP는 유효한 경로를 찾을 때까지 지정된 순서대로 경로를 시도합니다.

• \* 디렉토리 \*

사용자를 위해 생성한 사용자의 홈 디렉토리입니다. 디렉터리 이름은 일반적으로 사용자의 이름입니다. 검색 경로로 정의된 디렉토리 중 하나에 홈 디렉토리를 생성해야 합니다.

예를 들어, 다음 설정을 고려합니다.

- 사용자: John Smith
- 사용자 도메인: Acme
- 사용자 이름: jsmith
- SVM 이름: vs1
- 홈 디렉토리 공유 이름 #1: home\_""%w" - 공유 경로: "%w"
- 홈 디렉토리 공유 이름 #2:"%w" - 공유 경로: "%d/%w"
- 검색 경로 #1:'/vol0home/home'
- 검색 경로 #2:'/vol1home/home'
- 검색 경로 #3:'/vol2home/home'
- 홈 디렉토리: '/vol1home/home/jsmith'

시나리오 1: 사용자가 '\\VS1\home\_jsmith'에 연결합니다. 첫 번째 홈 디렉토리 공유 이름과 일치하고 상대 경로 jsmith를 생성합니다. ONTAP는 이제 각 검색 경로를 순서대로 확인하여 jsmith라는 디렉토리를 검색합니다.

- '/vol0home/home/jsmith'가 존재하지 않아 2번 검색경로로 이동함.
- '/vol1home/home/jsmith'가 존재하므로 검색 경로 #3이 확인되지 않고 사용자가 홈 디렉토리에 연결되어 있습니다.

시나리오 2: 사용자가 '\\VS1\jsmith'에 연결합니다. 두 번째 홈 디렉토리 공유 이름과 일치하고 상대 경로 Acme/jsmith를 생성합니다. ONTAP은 이제 각 검색 경로를 순서대로 확인하여 "Acme/jsmith"라는 디렉토리를 검색합니다.

- '/vol0home/home/acme/jsmith'가 존재하지 않고 검색 경로 #2로 이동합니다.
- '/vol1home/home/acme/jsmith'가 존재하지 않고 검색 경로 #3으로 이동합니다.
- '/vol2home/home/acme/jsmith'가 존재하지 않아 홈 디렉토리가 존재하지 않아 연결이 실패합니다.

## 홈 디렉토리 공유

홈 디렉토리 공유를 추가합니다

SMB 홈 디렉토리 기능을 사용하려면 공유 속성에 포함된 홈 디렉토리 속성에 공유를 하나 이상 추가해야 합니다.

이 작업에 대해

'vserver cifs share create' 명령을 사용하여 공유를 생성할 때 홈 디렉토리 공유를 생성하거나 'vserver cifs share modify' 명령을 사용하여 언제든지 기존 공유를 홈 디렉토리 공유로 변경할 수 있습니다.

홈 디렉토리 공유를 생성하려면 공유를 생성하거나 수정할 때 '-share-properties' 옵션에 homedirectory 값을 포함해야 합니다. 사용자가 홈 디렉토리에 연결할 때 동적으로 확장되는 변수를 사용하여 공유 이름을 지정하고 경로를 공유할 수 있습니다. 경로에서 사용할 수 있는 변수는 각각 Windows 사용자 이름, 도메인 및 매핑된 UNIX 사용자 이름에 해당하는 "%w", "%d" 및 "%u"입니다.

단계

1. 홈 디렉토리 공유 추가: + 'vserver cifs share create -vserver\_vserver\_name\_-share-name\_share\_name\_-path\_path\_-share-properties homedirectory [...]'

'-vserver'vserver'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

'-share-name\_share-name\_'은 홈 디렉토리 공유 이름을 지정합니다.

공유 이름에 리터럴 문자열 '%w', '%u' 또는 '%d' 중 하나가 포함된 경우 필수 변수 중 하나가 포함된 것 외에도 ONTAP가 리터럴 문자열을 변수(예: "%w")로 취급하지 않도록 리터럴 문자열 앞에 %(percent) 문자를 입력해야 합니다.

- 공유 이름에는 '%w' 또는 '%u' 변수가 포함되어야 합니다.
- 공유 이름에는 "%d" 변수(예: "%d"/"%w") 또는 공유 이름의 정적 부분(예: home1\_""%w")이 추가로 포함될 수 있습니다.
- 관리자가 공유를 사용하여 다른 사용자의 홈 디렉토리에 연결하거나 사용자가 다른 사용자의 홈 디렉토리에 연결할 수 있도록 허용하는 경우 동적 공유 이름 패턴 앞에는 물결표(~)가 와야 합니다.

vserver cifs home-directory modify는 '-is-home-dirs-access-for-admin-enabled' 옵션을 true로 설정하거나 고급 옵션 '-is-home-dirs-access-for-public-enabled'를 true로 설정하여 이 액세스를 활성화하는 데 사용됩니다.

path는 홈 디렉토리의 상대 경로를 지정합니다.

'-share-properties homedirectory[,...]'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다.

심표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

1. 'vserver cifs share show' 명령을 사용하여 홈 디렉토리 공유를 성공적으로 추가했는지 확인하십시오.

예

다음 명령을 실행하면 "%w"라는 홈 디렉토리 공유가 생성됩니다. oplocks, browsable, changenotify 공유 속성은 homedir 공유 속성을 설정하는 것 외에도 설정됩니다.



이 예에서는 SVM의 모든 공유에 대한 출력을 표시하지 않습니다. 출력이 잘립니다.

```
cluster1::> vservers cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vservers cifs share show -vserver vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	%w	%w	oplocks	-	Everyone / Full
Control			browsable		
			changenotify		
			homedirectory		

관련 정보

[홈 디렉토리 검색 경로 추가](#)

[자동 노드 조회를 사용하기 위한 요구 사항 및 지침](#)

[사용자의 홈 디렉터리에 대한 액세스 가능성 관리](#)

홈 디렉토리 공유에는 고유한 사용자 이름이 필요합니다

공유를 동적으로 생성하려면 "%w"(Windows 사용자 이름) 또는 "%u"(UNIX 사용자 이름) 변수를 사용하여 홈 디렉토리 공유를 생성할 때 고유한 사용자 이름을 지정해야 합니다. 공유 이름이 사용자 이름에 매핑됩니다.

정적 공유 이름과 사용자 이름이 같을 때 다음 두 가지 문제가 발생할 수 있습니다.

- 사용자가 net view 명령을 사용하여 클러스터의 공유를 나열하면 동일한 사용자 이름의 공유 두 개가 표시됩니다.
- 사용자가 해당 공유 이름에 연결하면 사용자는 항상 정적 공유에 연결되어 있으며 동일한 이름으로 홈 디렉토리 공유에 액세스할 수 없습니다.

예를 들어 "administrator"라는 이름의 공유가 있고 "administrator" Windows 사용자 이름이 있습니다. 홈 디렉토리 공유를 만들고 해당 공유에 연결하면 ""administrator"" 홈 디렉토리 공유가 아니라 ""administrator"" 정적 공유에 연결됩니다.

다음 단계를 수행하여 중복된 공유 이름으로 문제를 해결할 수 있습니다.

- 사용자의 홈 디렉토리 공유와 더 이상 충돌하지 않도록 정적 공유의 이름을 바꿉니다.
- 사용자에게 더 이상 정적 공유 이름과 충돌하지 않도록 새 사용자 이름을 제공합니다.
- '%w' 매개 변수를 사용하는 대신 "'home'"과 같은 정적 이름으로 CIFS 홈 디렉토리 공유를 생성하여 공유 이름과 충돌하지 않도록 합니다.

업그레이드 후 정적 홈 디렉토리 공유 이름은 어떻게 됩니까

홈 디렉토리 공유 이름에는 "%w" 또는 "%u" 동적 변수가 포함되어야 합니다. 새로운 요구 사항으로 ONTAP 버전으로 업그레이드한 후 기존 정적 홈 디렉토리 공유 이름에 어떤 일이 발생할지 알고 있어야 합니다.

홈 디렉토리 구성에 정적 공유 이름이 포함되어 있고 ONTAP로 업그레이드하면 정적 홈 디렉토리 공유 이름이 변경되지 않으며 여전히 유효합니다. 그러나 "%w" 또는 "%u" 변수를 포함하지 않는 새 홈 디렉토리 공유는 생성할 수 없습니다.

이러한 변수 중 하나를 사용자의 홈 디렉토리 공유 이름에 포함하도록 요구하면 모든 공유 이름이 홈 디렉토리 구성에서 고유하도록 할 수 있습니다. 필요한 경우 정적 홈 디렉토리 공유 이름을 "%w" 또는 "%u" 변수가 포함된 이름으로 변경할 수 있습니다.

홈 디렉토리 검색 경로를 추가합니다

ONTAP SMB 홈 디렉토리를 사용하려면 하나 이상의 홈 디렉토리 검색 경로를 추가해야 합니다.

이 작업에 대해

'vserver cifs home-directory search-path add' 명령을 사용하여 홈 디렉토리 검색 경로를 추가할 수 있습니다.

'vserver cifs home-directory search-path add' 명령은 명령 실행 중에 '-path' 옵션에 지정된 경로를 확인합니다. 지정된 경로가 없으면 명령을 실행하면 계속할 것인지 여부를 묻는 메시지가 생성됩니다. 당신은 'y'나 'n'을 선택합니다. 계속하려면 y를 선택하면 ONTAP가 검색 경로를 생성합니다. 그러나 홈 디렉토리 구성에서 검색 경로를 사용하려면 먼저 디렉토리 구조를 만들어야 합니다. 계속하지 않도록 선택하면 명령이 실패하고 검색 경로가 생성되지 않습니다. 그런 다음 경로 디렉토리 구조를 생성하고 'vserver cifs home-directory search-path add' 명령을 다시 실행할 수 있습니다.

단계

1. 홈 디렉토리 검색 경로 'vserver cifs home-directory search-path add-vserver vs1 -path path path' 추가
2. 'vserver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.

예

다음 예에서는 SVM VS1 홈 디렉토리 구성에 경로 '/home1'을 추가합니다.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

다음 예에서는 SVM VS1 홈 디렉토리 구성에 경로 '/home2'를 추가하려고 합니다. 경로가 존재하지 않습니다. 계속하지 않도록 선택할 수 있습니다.

```
cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

## 관련 정보

### 홈 디렉토리 공유를 추가하는 중입니다

%w 및 %d 변수를 사용하여 홈 디렉토리 설정을 작성합니다

"%w" 및 "%d" 변수를 사용하여 홈 디렉토리 설정을 작성할 수 있습니다. 사용자는 동적으로 생성된 공유를 사용하여 홈 공유에 연결할 수 있습니다.

## 단계

1. 사용자의 홈 디렉토리를 포함할 qtree를 생성합니다: 'volume qtree create-vsriver vsriver\_name-qtree-path qtree\_path'
2. qtree가 올바른 보안 유형인 'volume qtree show'를 사용하는지 확인합니다
3. Qtree에서 원하는 보안 스타일을 사용하지 않는 경우 'volume qtree security' 명령을 사용하여 보안 스타일을 변경하십시오.
4. 홈 디렉토리 공유 추가: "vsriver cifs share create-vsriver vsriver-share-name %w-path %d/%w-share-properties homedir디렉토리[,...]"

'-vsriver'vsriver'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

'-share-name '%w'는 홈 디렉토리 공유 이름을 지정합니다. ONTAP는 각 사용자가 홈 디렉토리에 접속할 때 동적으로 공유 이름을 생성합니다. 공유 이름은 *WINDOWS\_USER\_NAME* 형식입니다.

'-path '%d/%w'는 홈 디렉토리의 상대 경로를 지정합니다. 상대 경로는 각 사용자가 자신의 홈 디렉토리에 접속할 때 동적으로 생성되며 *domain/windows\_user\_name* 형식이 됩니다.

'-share-properties homedir디렉토리 [,...]+'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다. 심표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

5. 'vsriver cifs share show' 명령을 사용하여 공유에 원하는 구성이 있는지 확인합니다.
6. 홈 디렉토리 검색 경로 'vsriver cifs home-directory search-path add-vsriver vsriver-path path path' 추가

'-vsriver\_vsriver-name\_'은 검색 경로를 추가할 CIFS 지원 SVM을 지정합니다.

'-path\_path\_'는 검색 경로에 대한 절대 디렉토리 경로를 지정합니다.

7. 'vsriver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.
8. 홈 디렉토리가 있는 사용자의 경우 홈 디렉토리를 포함하도록 지정된 qtree 또는 볼륨에 해당 디렉토리를

생성합니다.

예를 들어, '/vol/vol1/users' 경로와 생성할 디렉토리가 mydomain\user1인 사용자 이름으로 qtree를 생성한 경우 '/vol/vol1/users/mydomain/user1' 경로를 사용하여 디렉토리를 생성합니다.

/home1 에 마운트된 ""home1" 볼륨을 생성한 경우 "/home1/mydomain/user1" 경로를 사용하여 디렉토리를 생성합니다.

9. 드라이브를 매핑하거나 UNC 경로를 사용하여 연결하여 사용자가 홈 공유에 성공적으로 연결할 수 있는지 확인합니다.

예를 들어, mydomain\user1 사용자가 SVM VS1 에 있는 8단계에서 생성한 디렉토리에 연결하려는 경우 user1은 UNC 경로 "\\VS1\user1"을 사용하여 연결됩니다.

예

다음 예제의 명령은 다음과 같은 설정으로 홈 디렉토리 구성을 만듭니다.

- 공유 이름은 %W입니다
- 상대 홈 디렉토리 경로는 %d/%W입니다
- 홈 디렉토리 /home1 을 포함하는 데 사용되는 검색 경로는 NTFS 보안 스타일로 구성된 볼륨입니다.
- SVM VS1 에서 구성이 생성됩니다.

사용자가 Windows 호스트에서 홈 디렉토리에 액세스할 때 이 유형의 홈 디렉토리 구성을 사용할 수 있습니다. 또한 사용자가 Windows 및 UNIX 호스트에서 홈 디렉토리를 액세스할 때 이 유형의 구성을 사용할 수 있으며 파일 시스템 관리자는 Windows 기반 사용자 및 그룹을 사용하여 파일 시스템에 대한 액세스를 제어할 수 있습니다.



```

cluster::> vservers cifs share create -vservers vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vservers cifs share show -vservers vs1 -share-name %w

Vserver: vs1
Share: %w
CIFS Server NetBIOS Name: VS1
Path: %d/%w
Share Properties: oplocks
                  browsable
                  changenotify
                  homedirectory
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vservers cifs home-directory search-path add -vservers vs1 -path
/home1

cluster::> vservers cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1

```

## 관련 정보

[%u 변수를 사용하여 홈 디렉토리를 구성하는 중입니다](#)

[추가 홈 디렉토리 구성](#)

[SMB 사용자의 홈 디렉토리 경로에 대한 정보 표시](#)

**%u** 변수를 사용하여 홈 디렉토리를 구성하십시오

'%w' 변수를 사용하여 공유 이름을 지정하는 홈 디렉토리 구성을 만들 수 있지만 '%u' 변수를 사용하여 홈 디렉토리 공유의 상대 경로를 지정할 수 있습니다. 그런 다음 사용자는 홈 디렉토리의 실제 이름 또는 경로를 인식하지 않고 Windows 사용자 이름을 사용하여 생성된 동적 공유를 사용하여 홈 공유에 연결할 수 있습니다.

단계

1. 사용자의 홈 디렉토리를 포함할 qtree를 생성합니다: 'volume qtree create-vserver vservers\_name-qtree-path qtree\_path'
2. qtree가 올바른 보안 유형인 'volume qtree show'를 사용하는지 확인합니다
3. Qtree에서 원하는 보안 스타일을 사용하지 않는 경우 'volume qtree security' 명령을 사용하여 보안 스타일을 변경하십시오.
4. 홈 디렉토리 공유 추가: "vserver cifs share create-vserver vservers-share-name%w-path%u-share-properties homed디렉토리,...]"

'-vserver'vservers'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

'-share-name '%w'는 홈 디렉토리 공유 이름을 지정합니다. 공유 이름은 각 사용자가 홈 디렉토리에 접속하고 *mapped\_unix\_user\_name* 형식으로 작성될 때 동적으로 생성됩니다.



'-share-name' 옵션에도 '%u' 변수를 사용할 수 있습니다. 이렇게 하면 매핑된 UNIX 사용자 이름을 사용하는 상대 공유 경로가 생성됩니다.

'-path '%u'는 홈 디렉토리의 상대 경로를 지정합니다. 상대 경로는 각 사용자가 홈 디렉토리에 접속하고 *Mapped\_UNIX\_USER\_NAME* 형식으로 작성될 때 동적으로 생성됩니다.



이 옵션의 값에는 정적 요소도 포함될 수 있습니다. 예: 'ENG/%u'.

'-share-properties' + homed디렉토리 \[,...]\+'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다. 쉼표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

5. 'vserver cifs share show' 명령을 사용하여 공유에 원하는 구성이 있는지 확인합니다.
6. 홈 디렉토리 검색 경로 'vserver cifs home-directory search-path add-vserver vservers-path path path' 추가

'-vserver'vservers'는 검색 경로를 추가할 CIFS 지원 SVM을 지정합니다.

path는 검색경로에 대한 절대 디렉토리 경로를 지정합니다.

7. 'vserver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.
8. UNIX 사용자가 없으면 'vserver services UNIX -user create' 명령을 사용하여 UNIX 사용자를 생성합니다.



사용자를 매핑하기 전에 Windows 사용자 이름을 매핑할 UNIX 사용자 이름이 있어야 합니다.

9. "vserver name-mapping create -vserver vservers\_name -direction win -unix -priority integer -pattern windows\_user\_name -replacement unix\_user\_name" 명령을 사용하여 UNIX 사용자에 대한 Windows 사용자의 이름 매핑을 생성합니다



Windows 사용자를 UNIX 사용자에게 매핑하는 이름 매핑이 이미 있는 경우 매핑 단계를 수행할 필요가 없습니다.

Windows 사용자 이름이 해당 UNIX 사용자 이름으로 매핑됩니다. Windows 사용자가 홈 디렉토리 공유에 접속하면 디렉토리 이름이 UNIX 사용자 이름과 일치한다는 것을 인식하지 않고 동적으로 생성된 홈 디렉토리에 Windows 사용자 이름에 해당하는 공유 이름을 연결합니다.

10. 홈 디렉토리가 있는 사용자의 경우 홈 디렉토리를 포함하도록 지정된 qtree 또는 볼륨에 해당 디렉토리를 생성합니다.

예를 들어, 생성하려는 디렉토리가 `"/home1/unixuser1"`인 사용자의 매핑된 UNIX 사용자 이름과 함께 `"/vol/vol1/users"` 경로를 사용하여 qtree를 생성한 경우 `"/vol/vol1/users/unixuser1"` 경로를 사용하여 디렉토리를 생성할 수 있습니다.

`/home1`에 마운트된 `"/home1"` 볼륨을 생성한 경우 `"/home1/unixuser1"` 경로를 사용하여 디렉토리를 생성합니다.

11. 드라이브를 매핑하거나 UNC 경로를 사용하여 연결하여 사용자가 홈 공유에 성공적으로 연결할 수 있는지 확인합니다.

예를 들어, 사용자 `mydomain\user1`이 UNIX 사용자 `unixuser1`에 매핑되고 SVM VS1에 있는 10단계에서 생성한 디렉토리에 연결하려는 경우 `user1`은 UNC 경로 `"\\VS1\user1"`을 사용하여 연결됩니다.

예

다음 예제의 명령은 다음과 같은 설정으로 홈 디렉토리 구성을 만듭니다.

- 공유 이름은 `%W`입니다
- 상대 홈 디렉토리 경로는 `%u`입니다
- 홈 디렉토리 `/home1`을 포함하는 데 사용되는 검색 경로는 UNIX 보안 스타일로 구성된 볼륨입니다.
- SVM VS1에서 구성이 생성됩니다.

사용자가 Windows 호스트 또는 Windows 및 UNIX 호스트 모두에서 홈 디렉토리에 액세스할 때 이 유형의 홈 디렉토리 구성을 사용할 수 있으며 파일 시스템 관리자는 UNIX 기반 사용자 및 그룹을 사용하여 파일 시스템에 대한 액세스를 제어할 수 있습니다.

```
cluster::> vservice cifs share create -vservice vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vservice cifs share show -vservice vs1 -share-name %u
```

```

                Vservice: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
        Share Properties: oplocks
                        browsable
                        changenotify
                        homedirectory
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vservice cifs home-directory search-path add -vservice vs1 -path
/home1
```

```
cluster::> vservice cifs home-directory search-path show -vservice vs1
```

```
Vservice      Position Path
-----
vs1            1        /home1
```

```
cluster::> vservice name-mapping create -vservice vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vservice name-mapping show -pattern user1
```

```
Vservice      Direction Position
-----
vs1            win-unix  5        Pattern: user1
                                Replacement: unixuser1
```

## 관련 정보

[%w 및 %d 변수를 사용하여 홈 디렉토리 설정을 작성합니다](#)

[추가 홈 디렉토리 구성](#)

## SMB 사용자의 홈 디렉토리 경로에 대한 정보 표시

### 추가 홈 디렉토리 구성

"%w", "%d", "%u" 변수를 사용하여 홈 디렉토리 설정을 추가로 생성할 수 있습니다. 이 변수를 사용하여 필요에 맞게 홈 디렉토리 구성을 사용자 정의할 수 있습니다.

공유 이름과 검색 경로에서 변수와 정적 문자열을 조합하여 여러 홈 디렉토리 구성을 만들 수 있습니다. 다음 표에는 여러 가지 홈 디렉토리 구성을 만드는 방법을 보여 주는 몇 가지 예가 나와 있습니다.

'vol1/user'가 홈 디렉토리를 포함할 때 생성되는 경로...	공유 명령...
사용자를 'vol1/user/win_username'으로 안내하는 공유 경로 '\\vs1\~win_username'을 만듭니다	'vserver cifs share create-share-name~%w-path%w-share-properties oplocks, browsable, changenotify, homedir'
사용자를 'vol1/user/domain/win_username'으로 안내하는 공유 경로 '\\vs1\win_username'을 만듭니다	'vserver cifs share create-share-name %w-path %d/%w-share-properties oplocks, browsable, changenotify, homedir'
사용자를 'vol1/user/unix_username'으로 안내하는 공유 경로 '\\vs1\win_username'을 만듭니다	'vserver cifs share create-share-name %w-path %u-share-properties oplocks, browsable, changenotify, homedir'
사용자를 'vol1/user/unix_username'으로 안내하는 공유 경로 '\\vs1\unix_username'을 생성합니다	'vserver cifs share create-share-name %u-path %u-share-properties oplocks, browsable, changenotify, homedir'

검색 경로 관리를 위한 명령입니다

SMB 홈 디렉토리 구성을 위한 검색 경로를 관리하기 위한 특정 ONTAP 명령이 있습니다. 예를 들어, 검색 경로에 대한 정보를 추가, 제거 및 표시하는 명령이 있습니다. 검색 경로 순서를 변경하는 명령도 있습니다.

원하는 작업	이 명령 사용...
검색 경로를 추가합니다	'vserver cifs home-directory search-path add'
검색 경로를 표시합니다	'vserver cifs home-directory search-path show'
검색 경로 순서를 변경합니다	'vserver cifs home-directory search-path reorder'
검색 경로를 제거합니다	'vserver cifs home-directory search-path remove'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

**SMB** 사용자의 홈 디렉토리 경로에 대한 정보를 표시합니다

스토리지 가상 시스템(SVM)에 SMB 사용자의 홈 디렉토리 경로를 표시할 수 있습니다. SVM은 CIFS 홈 디렉토리 경로가 여러 개 구성되어 있고 사용자의 홈 디렉토리가 있는 경로를 확인하려는 경우에 사용할 수 있습니다.

단계

1. 'vserver cifs home-directory show-user' 명령을 사용하여 홈 디렉토리 경로를 표시합니다.

```
'vserver cifs home-directory show-user-vserver vs1-username user1'
```

Vserver	User	Home Dir Path
vs1	user1	/home/user1

관련 정보

[사용자의 홈 디렉터리에 대한 액세스 가능성 관리](#)

사용자의 홈 디렉터리에 대한 액세스 권한을 관리합니다

기본적으로 사용자의 홈 디렉토리는 해당 사용자만 액세스할 수 있습니다. 공유의 동적 이름 앞에 물결표(~)가 있는 공유의 경우 Windows 관리자 또는 다른 사용자(공용 액세스)가 사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제할 수 있습니다.

시작하기 전에

SVM(스토리지 가상 머신)의 홈 디렉토리 공유는 앞에 물결표(~)가 오는 동적 공유 이름으로 구성해야 합니다. 다음 사례는 공유 명명 요구 사항을 보여 줍니다.

홈 디렉토리 공유 이름입니다	공유에 연결하는 명령의 예
~ %d~ %w	'net use * {백슬래시} {백슬래시}IPaddress{백슬래시} ~domain~user/u:credentials'을 사용하십시오
~ %w	'net use * {백슬래시} {백슬래시}IPaddress{백슬래시} ~user/u:credentials'를 사용하십시오
~abc~ %w	'net use * {백슬래시} {백슬래시}IPaddress{백슬래시}abc~user/u:credentials'를 사용하십시오

단계

1. 적절한 작업을 수행합니다.

사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제하려면...	다음을 입력하십시오.
Windows 관리자	'vserver cifs home-directory modify -vserver_vserver_name_-is-home-dirs-access-for-admin-enabled{true false}' 기본값은 'true'입니다.
모든 사용자(공용 액세스)	a. 권한 수준을 advanced:+'et-Privilege advanced'로 설정합니다 b. 액세스 설정 또는 해제:'vserver cifs home-directory modify -vserver_vserver_name_-is-home-dirs-access-for-public-enabled{true

다음 예에서는 사용자의 홈 디렉토리에 대한 공용 액세스를 활성화합니다. + 'Set-Privilege advanced' + 'vserver cifs home-directory modify -vserver vs1-is-home-dirs-access-for-public-enabled true' + 'Set-Privilege admin'

관련 정보

[SMB 사용자의 홈 디렉토리 경로에 대한 정보 표시](#)

## UNIX 심볼 링크에 대한 SMB 클라이언트 액세스를 구성합니다

ONTAP를 통해 UNIX 심볼 링크에 대한 SMB 클라이언트 액세스를 제공하는 방법

심볼 링크는 다른 파일 또는 디렉토리에 대한 참조가 포함된 UNIX 환경에서 생성되는 파일입니다. 클라이언트가 심볼 링크에 액세스하는 경우 클라이언트는 심볼 링크가 참조하는 타겟 파일 또는 디렉토리로 리디렉션됩니다. ONTAP는 Wwidelink(로컬 파일 시스템 외부의 타겟을 포함한 절대 링크)를 포함하여 상대 및 절대 심볼 링크를 지원합니다.

ONTAP는 SMB 클라이언트가 SVM에 구성된 UNIX 심볼 링크를 따라갈 수 있도록 지원합니다. 이 기능은 선택 사항이며 다음 설정 중 하나로 'vserver cifs share create' 명령의 '-symlink-properties' 옵션을 사용하여 공유별로 구성할 수 있습니다.

- 읽기/쓰기 권한으로 설정됩니다
- 읽기 전용 액세스를 사용하도록 설정되었습니다
- SMB 클라이언트에서 심볼 링크를 숨겨 사용할 수 없습니다
- SMB 클라이언트의 심볼 링크에 대한 액세스 없이 비활성화됩니다

공유에 대한 심볼 링크를 설정하면 추가 구성 없이 상대 심볼 링크가 작동합니다.

공유에 대한 심볼 링크를 설정하면 절대 심볼 링크가 즉시 작동하지 않습니다. 먼저 대상 SMB 경로에 대한 심볼 링크의 UNIX 경로 간에 매핑을 생성해야 합니다. 절대 심볼 링크 매핑을 생성할 때 로컬 링크인지 또는 \_wwidelink\_ 인지를 지정할 수 있습니다. widelink는 다른 스토리지 디바이스의 파일 시스템에 대한 링크이거나 동일한 ONTAP 시스템에서 별도의 SVM에 호스팅된 파일 시스템에 대한 링크일 수 있습니다. widelink를 만들 때는 클라이언트가 따라야 하는 정보를 포함해야 합니다. 즉, 클라이언트가 디렉터리 연결 지점을 검색할 재분석 지점을 만들어야 합니다. 로컬 공유 외부에 있는 파일 또는 디렉토리에 대한 절대 심볼 링크를 생성하지만 인접성을 로컬로 설정하면 ONTAP는 타겟에 대한 액세스를 허용하지 않습니다.



클라이언트가 로컬 심볼 링크(절대 또는 상대 링크)를 삭제하려고 하면 타겟 파일이나 디렉토리가 아닌 심볼 링크만 삭제됩니다. 그러나 클라이언트가 widelink를 삭제하려고 하면 wwidelink가 참조하는 실제 타겟 파일이나 디렉토리가 삭제될 수 있습니다. 클라이언트가 SVM 외부에서 타겟 파일 또는 디렉토리를 명시적으로 열고 삭제할 수 있기 때문에 ONTAP에서는 이 기능을 제어할 수 없습니다.

• \* 재분석 지점 및 ONTAP 파일 시스템 서비스 \*

reparse point\_는 파일과 함께 볼륨에 선택적으로 저장할 수 있는 NTFS 파일 시스템 객체입니다. 재분석 지점은 SMB 클라이언트가 NTFS 스타일 볼륨으로 작업할 때 향상된 파일 시스템 서비스 또는 확장된 파일 시스템 서비스를 받을 수 있는 기능을 제공합니다. 재분석 지점은 재분석 지점의 유형을 식별하는 표준 태그 및 클라이언트가 추가 처리를 위해 SMB 클라이언트에서 검색할 수 있는 재분석 지점의 콘텐츠로 구성됩니다. 확장된 파일 시스템 기능에 사용할 수 있는 개체 유형 중 ONTAP는 재분석 포인트 태그를 사용하여 NTFS 심볼 링크 및 디렉터리 연결 지점에 대한 지원을 구현합니다. 재분석 지점의 내용을 이해할 수 없는 SMB 클라이언트는 단순히 무시하며 재분석 지점에서 활성화할 수 있는 확장 파일 시스템 서비스를 제공하지 않습니다.

• \* 심볼 링크에 대한 디렉터리 교차점 및 ONTAP 지원 \*

디렉터리 교차점은 파일이 저장된 대체 위치를 다른 경로(심볼 링크) 또는 별도의 스토리지 디바이스(widelinks)에 참조할 수 있는 파일 시스템 디렉터리 구조 내의 위치입니다. ONTAP SMB 서버는 디렉터리 연결 지점을 재분석 지점으로 Windows 클라이언트에 노출하므로, 디렉터리 연결 지점을 이동할 때 사용 가능한 클라이언트가 ONTAP에서 재분석 지점 내용을 가져올 수 있습니다. 따라서 동일한 파일 시스템에 포함된 것처럼 다른 경로 또는 스토리지 디바이스를 탐색하고 연결할 수 있습니다.

• \* 재분석 포인트 옵션을 사용하여 widelink 지원 활성화 \*

ONTAP 9에서는 기본적으로 '-is-use-junction-as-reparse-points-enabled' 옵션이 활성화됩니다. 모든 SMB 클라이언트가 wirelink를 지원하는 것은 아니므로 정보를 활성화하는 옵션은 프로토콜 버전별로 구성할 수 있으므로 관리자가 지원되는 SMB 클라이언트와 지원되지 않는 SMB 클라이언트를 모두 수용할 수 있습니다. ONTAP 9.2 이상의 릴리즈에서는 wdelink를 사용하여 공유에 액세스하는 각 클라이언트 프로토콜에 대해 '-wirelink-as-reparse-point-versions' 옵션을 활성화해야 합니다. 기본값은 SMB1입니다. 이전 릴리즈에서는 기본 SMB1을 사용하여 액세스되는 Wodelink만 보고되었으며 SMB2 또는 SMB3을 사용하는 시스템에서는 wdelink에 액세스할 수 없었습니다.

자세한 내용은 Microsoft NTFS 설명서를 참조하십시오.

["Microsoft 설명서: 지점 재분석"](#)

**SMB 액세스에 대한 UNIX 심볼 링크를 구성할 때의 제한**

SMB 액세스를 위해 UNIX 심볼 링크를 구성할 때 특정 제한 사항을 알고 있어야 합니다.

제한	설명
45	<p>CIFS 서버 이름에 FQDN을 사용할 때 지정할 수 있는 CIFS 서버 이름의 최대 길이입니다.</p> <div>  <p>또는 CIFS 서버 이름을 NetBIOS 이름으로 지정할 수 있습니다. 이 이름은 15자로 제한됩니다.</p> </div>



제한	설명
80	공유 이름의 최대 길이입니다.
256	심볼 링크를 생성할 때 또는 기존 심볼 링크의 UNIX 경로를 수정할 때 지정할 수 있는 UNIX 경로의 최대 길이입니다. UNIX 경로는 "/"(슬래시)로 시작하고 "/"로 끝나야 합니다. 시작 및 끝 슬래시는 모두 256자 제한의 일부로 계산됩니다.
256	심볼 링크를 생성하거나 기존 심볼 링크의 CIFS 경로를 수정할 때 지정할 수 있는 CIFS 경로의 최대 길이입니다. CIFS 경로는 "/"(슬래시)로 시작하고 "/"로 끝나야 합니다. 시작 및 끝 슬래시는 모두 256자 제한의 일부로 계산됩니다.

#### 관련 정보

#### SMB 공유에 대한 심볼 링크 매핑 생성

**CIFS** 서버 옵션을 사용하여 **ONTAP**에서 자동 **DFS** 광고를 제어합니다

CIFS 서버 옵션은 공유에 연결할 때 SMB 클라이언트에 DFS 기능을 알리는 방법을 제어합니다. ONTAP는 클라이언트가 SMB를 통해 심볼 링크에 액세스할 때 DFS 조회를 사용하므로 이 옵션을 비활성화하거나 활성화할 때 어떤 영향이 있는지 알고 있어야 합니다.

CIFS 서버 옵션은 CIFS 서버가 SMB 클라이언트에 DFS를 사용할 수 있음을 자동으로 알리는지 여부를 결정합니다. 기본적으로 이 옵션은 설정되어 있으며 CIFS 서버는 심볼 링크에 대한 액세스가 비활성화된 공유에 연결할 때도 SMB 클라이언트에 DFS를 사용할 수 있다고 항상 알립니다. CIFS 서버가 심볼 링크에 대한 액세스가 설정된 공유에 연결할 때만 DFS를 클라이언트에 제공할 수 있음을 알려려면 이 옵션을 사용하지 않도록 설정할 수 있습니다.

이 옵션을 비활성화하면 어떻게 되는지 알고 있어야 합니다.

- 심볼 링크에 대한 공유 구성은 변경되지 않습니다.
- 공유 매개 변수가 심볼 링크 액세스를 허용하도록 설정된 경우(읽기-쓰기 액세스 또는 읽기 전용 액세스) CIFS 서버는 해당 공유에 접속하는 클라이언트에 DFS 기능을 알립니다.

클라이언트 연결 및 심볼 링크에 대한 액세스는 중단 없이 계속됩니다.

- 공유 매개 변수가 액세스를 비활성화하거나 공유 매개 변수의 값이 null인 경우 심볼 링크 액세스를 허용하지 않도록 설정된 경우 CIFS 서버는 해당 공유에 접속하는 클라이언트에 DFS 기능을 알리지 않습니다.

클라이언트는 CIFS 서버가 DFS를 사용할 수 있고 더 이상 DFS를 광고하지 않기 때문에 심볼 링크 액세스가 비활성화된 공유에 접속된 클라이언트는 CIFS 서버 옵션을 비활성화한 후 이러한 공유에 액세스하지 못할 수 있습니다. 이 옵션을 사용하지 않도록 설정한 후 이러한 공유에 연결된 클라이언트를 재부팅해야 캐시된 정보가 지워질 수 있습니다.

이러한 변경 사항은 SMB 1.0 연결에는 적용되지 않습니다.

## SMB 공유에 대한 UNIX 심볼 링크 지원을 구성합니다

SMB 공유를 생성할 때 또는 언제든지 기존 SMB 공유를 수정하여 심볼 링크 공유 속성 설정을 지정하여 SMB 공유에 대한 UNIX 심볼 링크 지원을 구성할 수 있습니다. UNIX 심볼 링크 지원은 기본적으로 활성화되어 있습니다. 공유에서 UNIX 심볼 링크 지원을 해제할 수도 있습니다.

이 작업에 대해

SMB 공유에 대한 UNIX 심볼 링크 지원을 구성할 때 다음 설정 중 하나를 선택할 수 있습니다.

설정	설명
'enable'(사용되지 않음 *)	심볼 링크가 읽기-쓰기 액세스를 사용하도록 설정되도록 지정합니다.
READ_ONLY'(사용되지 않음 *)	읽기 전용 액세스를 위해 symlink를 사용하도록 지정합니다. 이 설정은 Wodelink에는 적용되지 않습니다. Widelink 액세스는 항상 읽기-쓰기입니다.
'hide'(사용되지 않음 *)	SMB 클라이언트가 symlink를 볼 수 없도록 지정합니다.
엄정한 보안 없음	클라이언트가 공유 경계 외부의 symlink를 따르도록 지정합니다.
'체조'입니다	symlink가 읽기-쓰기 액세스를 위해 로컬로 설정되도록 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 true로 설정되어 있어도 DFS 광고는 생성되지 않습니다. 기본 설정입니다.
'체임링크', '와이델링크'	읽기-쓰기 액세스를 위해 로컬 symlink와 wizenlink를 모두 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 false로 설정되어 있어도 로컬 symlink와 Wipelink 모두에 대해 DFS 광고가 생성됩니다.
"할 수 없습니다	symlinks 및 widelinks를 사용하지 않도록 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 true로 설정되어 있어도 DFS 광고는 생성되지 않습니다.
""(null, 설정되지 않음)	공유의 심볼 링크를 해제합니다.
'-(설정되지 않음)	공유의 심볼 링크를 해제합니다.



- enable\_, hide 및 \_read-only\_parameters는 더 이상 사용되지 않으며 ONTAP의 향후 릴리스에서 제거될 수 있습니다.

단계

1. 심볼 링크 지원을 구성하거나 사용하지 않도록 설정:

만약...	입력...
새로운 SMB 공유	'+vserver cifs share create-vserver vserver_name-share-name share-path-path-symlink-properties{enable
hide	read-only
""	-
symlinks	symlinks-and-wdelink
disable},...]+'	기존 SMB 공유입니다
'+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink -properties{enable	hide
read-only	"
-	symlinks
symlinks-and-wifelink	disable},...]+'

2. SMB 공유 구성이 올바른지 확인합니다. 'vserver cifs share show -vserver vserver\_name -share-name share\_name -instance'

예

다음 명령을 실행하면 UNIX 심볼 링크 구성이 "enable"로 설정된 "data1"이라는 SMB 공유가 생성됩니다.

```
cluster1::> vsserver cifs share create -vsserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

## 관련 정보

### [SMB 공유에 대한 심볼 링크 매핑 생성](#)

#### **SMB** 공유에 대한 심볼 링크 매핑을 생성합니다

SMB 공유에 대한 UNIX 심볼 링크 매핑을 생성할 수 있습니다. 상위 폴더에 상대적인 파일이나 폴더를 참조하는 상대 심볼 링크를 만들거나 절대 경로를 사용하여 파일 또는 폴더를 참조하는 절대 심볼 링크를 만들 수 있습니다.

#### 이 작업에 대해

SMB 2.x를 사용하는 경우 Mac OS X 클라이언트에서 Widelink에 액세스할 수 없습니다 사용자가 Mac OS X 클라이언트의 widelink를 사용하여 공유에 연결하려고 하면 시도가 실패합니다. 그러나 SMB 1을 사용하는 경우 Mac OS X 클라이언트에서 Wistelink를 사용할 수 있습니다.

#### 단계

1. SMB 공유에 대한 심볼 링크 매핑을 생성하려면 다음을 수행합니다. "vsserver cifs symlink create -vsserver virtual\_server\_name -unix-path path path path -share-name share\_name -cifs-path path path path[-cifs-server server\_name][-locality{local|free|wdelink}][-home-directory{true|false}]"

'-vsserver'virtual\_server\_name'은 SVM(Storage Virtual Machine) 이름을 지정합니다.

'-unix-path' path는 UNIX 경로를 지정합니다. UNIX 경로는 슬래시("/")로 시작해야 하며 슬래시("/")로 끝나야 합니다.

'-share-name' share\_name'은 매핑할 SMB 공유의 이름을 지정합니다.

'-cifs-path' path는 CIFS 경로를 지정합니다. CIFS 경로는 슬래시("/")로 시작해야 하며 슬래시("/")로 끝나야 합니다.

'-cifs-server "server\_name'은 CIFS 서버 이름을 지정합니다. CIFS 서버 이름은 DNS 이름(예: mynetwork.cifs.server.com), IP 주소 또는 NetBIOS 이름으로 지정할 수 있습니다. NetBIOS 이름은 'vserver cifs show' 명령을 사용하여 확인할 수 있습니다. 이 선택적 매개 변수를 지정하지 않으면 로컬 CIFS 서버의 NetBIOS 이름이 기본값이 됩니다.

'-locality' {'local'|'free'|'widelink'}은 로컬 링크, 무료 링크 또는 넓은 심볼 링크 생성 여부를 지정합니다. 로컬 심볼 링크는 로컬 SMB 공유에 매핑됩니다. 무료 심볼 링크는 로컬 SMB 서버의 어느 위치에나 매핑할 수 있습니다. 넓은 심볼 링크는 네트워크의 모든 SMB 공유에 매핑됩니다. 이 선택적 매개 변수를 지정하지 않으면 기본값은 "local"입니다.

'-home-directory' {'true'|'false'}는 타겟 공유가 홈 디렉토리인지 여부를 지정합니다. 이 매개 변수는 선택 사항이지만 타겟 공유가 홈 디렉토리로 구성될 때 이 매개 변수를 "true"로 설정해야 합니다. 기본값은 false 입니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 심볼 링크 매핑이 생성됩니다. UNIX 경로인 /src/, SMB 공유 이름 "소스", CIFS 경로, /mycompany/source/", CIFS 서버 IP 주소 123.123.123.123 등이 있으며, 이는 wizenlink입니다.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

관련 정보

[SMB 공유에서 UNIX 심볼 링크 지원 구성](#)

심볼 링크 매핑을 관리하는 명령입니다

심볼 링크 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
심볼 링크 매핑을 생성합니다	'vserver cifs symlink create
심볼 링크 매핑에 대한 정보를 표시합니다	'vserver cifs symlink show'
심볼 링크 매핑을 수정합니다	'vserver cifs symlink modify'
심볼 링크 매핑을 삭제합니다	'vserver cifs symlink delete

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

## BranchCache를 사용하여 지사에 SMB 공유 콘텐츠를 캐싱합니다

BranchCache를 사용하여 지사 개요에서 SMB 공유 콘텐츠를 캐시합니다

BranchCache는 요청 클라이언트에 대한 로컬 컴퓨터의 콘텐츠를 캐싱할 수 있도록 Microsoft에서 개발했습니다. ONTAP의 BranchCache를 구현하면 WAN(Wide Area Network) 사용률을 줄이고, 지사의 사용자가 SMB를 사용하여 SVM(Storage Virtual Machine)에 저장된 콘텐츠에 액세스할 때 액세스 응답 시간을 향상시킬 수 있습니다.

BranchCache를 구성하는 경우 Windows BranchCache 클라이언트는 먼저 SVM에서 콘텐츠를 검색한 다음 지사 내의 컴퓨터에 콘텐츠를 캐시합니다. 지사의 다른 BranchCache 지원 클라이언트가 동일한 콘텐츠를 요청하는 경우 SVM은 먼저 요청된 사용자를 인증하고 권한을 부여합니다. 그런 다음, SVM이 캐시된 콘텐츠가 아직 최신 상태인지 확인하고 최신 상태인 경우 캐시된 콘텐츠에 대한 클라이언트 메타데이터를 보냅니다. 그런 다음 클라이언트는 메타데이터를 사용하여 로컬 기반 캐시에서 콘텐츠를 직접 검색합니다.

### 관련 정보

[오프라인 파일을 사용하여 오프라인 사용을 위해 파일 캐싱을 허용합니다](#)

### 요구사항 및 지침

#### BranchCache 버전 지원

ONTAP가 지원하는 BranchCache 버전은 무엇인지 알고 있어야 합니다.

ONTAP는 BranchCache 1 및 향상된 BranchCache 2를 지원합니다.

- SVM(스토리지 가상 시스템)에 대해 SMB 서버의 BranchCache를 구성할 때 BranchCache 1, BranchCache 2 또는 모든 버전을 사용하도록 설정할 수 있습니다.

기본적으로 모든 버전이 활성화됩니다.

- BranchCache 2만 사용하도록 설정한 경우 원격 사무소 Windows 클라이언트 시스템은 BranchCache 2를 지원해야 합니다.

SMB 3.0 이상 클라이언트만 BranchCache 2를 지원합니다.

BranchCache 버전에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

### 관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

#### 네트워크 프로토콜 지원 요구 사항

ONTAP BranchCache를 구축하기 위한 네트워크 프로토콜 요구 사항을 알고 있어야 합니다.

SMB 2.1 이상을 사용하여 IPv4 및 IPv6 네트워크에서 ONTAP BranchCache 기능을 구현할 수 있습니다.

BranchCache 구축에 사용되는 모든 CIFS 서버 및 지사 시스템에는 SMB 2.1 이상 프로토콜이 설정되어 있어야 합니다. SMB 2.1에는 클라이언트가 BranchCache 환경에 참여할 수 있도록 하는 프로토콜 확장이 있습니다. BranchCache 지원을 제공하는 최소 SMB 프로토콜 버전입니다. SMB 2.1은 BranchCache 버전 1을 지원합니다.

BranchCache 버전 2를 사용하려면 SMB 3.0이 지원되는 최소 버전입니다. BranchCache 2 구축에 사용되는 모든 CIFS 서버 및 지사 시스템에는 SMB 3.0 이상이 활성화되어 있어야 합니다.

일부 클라이언트가 SMB 2.1만 지원하고 일부 클라이언트가 SMB 3.0을 지원하는 원격 사무소가 있는 경우 CIFS 서버에 BranchCache 1과 BranchCache 2를 모두 지원하는 BranchCache 구성을 구현할 수 있습니다.



Microsoft BranchCache 기능은 HTTP/HTTPS 및 SMB 프로토콜을 파일 액세스 프로토콜로 사용하는 것을 지원하지만 ONTAP BranchCache는 SMB의 사용만 지원합니다.

#### ONTAP 및 Windows 호스트 버전 요구 사항

BranchCache를 구성하려면 ONTAP 및 지점 Windows 호스트가 특정 버전 요구 사항을 충족해야 합니다.

BranchCache를 구성하기 전에 클러스터 및 참여하는 지사 클라이언트의 ONTAP 버전이 SMB 2.1 이상을 지원하고 BranchCache 기능을 지원해야 합니다. Hosted Cache 모드를 구성하는 경우 캐시 서버에 지원되는 호스트를 사용해야 합니다.

BranchCache 1은 다음 ONTAP 버전 및 Windows 호스트에서 지원됩니다.

- 콘텐츠 서버: ONTAP 기반의 SVM(스토리지 가상 시스템)
- 캐시 서버: Windows Server 2008 R2 또는 Windows Server 2012 이상
- 피어 또는 클라이언트: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 또는 Windows Server 2012 이상

BranchCache 2는 다음 ONTAP 버전 및 Windows 호스트에서 지원됩니다.

- 콘텐츠 서버: ONTAP 기반의 SVM
- 캐시 서버: Windows Server 2012 이상
- 피어 또는 클라이언트: Windows 8 또는 Windows Server 2012 이상

#### ONTAP가 BranchCache 해시를 무효화하는 이유

BranchCache 구성을 계획할 때 ONTAP에서 해시를 무효화하는 이유를 이해하는 것이 도움이 될 수 있습니다. 구성할 운영 모드를 결정하는 데 도움이 되며 BranchCache를 활성화할 공유를 선택하는 데 도움이 될 수 있습니다.

ONTAP는 해시가 유효한지 확인하기 위해 BranchCache 해시를 관리해야 합니다. 해시가 유효하지 않은 경우 ONTAP는 해시를 무효화하고 다음에 해당 콘텐츠가 요청될 때 BranchCache가 여전히 활성화되어 있다고 가정하고 새 해시를 계산합니다.

ONTAP는 다음과 같은 이유로 해시를 무효화합니다.

- 서버 키가 수정되었습니다.

서버 키가 수정되면 ONTAP는 해시 저장소의 모든 해시를 무효화합니다.

- BranchCache 해시 저장소의 최대 크기에 도달했기 때문에 캐시에서 해시가 플러시됩니다.

이 매개 변수는 조정 가능하며 비즈니스 요구 사항에 맞게 수정할 수 있습니다.

- 파일은 SMB 또는 NFS 액세스를 통해 수정됩니다.
- 해시가 계산된 파일은 'Snap restore' 명령어를 이용하여 복구한다.
- BranchCache를 사용하는 SMB 공유가 포함된 볼륨은 'Snap restore' 명령을 사용하여 복구됩니다.

#### 해시 저장 위치 선택 지침

BranchCache를 구성할 때는 해시를 저장할 위치와 해시 저장소의 크기를 선택합니다. 해시 저장소 위치 및 크기를 선택할 때 지침을 이해하면 CIFS 지원 SVM에서 BranchCache 구성을 계획하는 데 도움이 됩니다.

- atime 업데이트가 허용되는 볼륨에서 해시 저장소를 찾아야 합니다.

해시 파일의 액세스 시간은 자주 액세스하는 파일을 해시 저장소에 유지하는 데 사용됩니다. atime 업데이트가 비활성화된 경우 생성 시간이 이 용도로 사용됩니다. 자주 사용하는 파일을 추적하기 위해 atime을 사용하는 것이 좋습니다.

- SnapMirror 대상 및 SnapLock 볼륨과 같은 읽기 전용 파일 시스템에서는 해시를 저장할 수 없습니다.
- 해시 저장소의 최대 크기에 도달하면 새 해시를 위한 공간을 확보하기 위해 이전 해시가 플러시됩니다.

해시 저장소의 최대 크기를 늘려 캐시에서 플러시되는 해시의 양을 줄일 수 있습니다.

- 해시를 저장하는 볼륨을 사용할 수 없거나 꽉 찼거나 BranchCache 서비스에서 해시 정보를 검색할 수 없는 클러스터 내 통신에 문제가 있는 경우 BranchCache 서비스를 사용할 수 없습니다.

볼륨이 오프라인 상태이거나 스토리지 관리자가 해시 저장소에 대한 새 위치를 지정했기 때문에 볼륨을 사용할 수 없습니다.

이 경우 파일 액세스에 문제가 발생하지 않습니다. 해시 저장소에 대한 액세스가 방해받으면 ONTAP는 클라이언트에 Microsoft 정의 오류를 반환하여 클라이언트가 일반 SMB 읽기 요청을 사용하여 파일을 요청하게 합니다.

#### 관련 정보

[SMB 서버에서 BranchCache를 구성합니다](#)

[BranchCache 구성을 수정합니다](#)

#### BranchCache 권장 사항

BranchCache를 구성하기 전에 BranchCache 캐싱을 활성화할 SMB 공유를 결정할 때 유의해야 할 몇 가지 권장 사항이 있습니다.

사용할 운영 모드와 BranchCache를 활성화할 SMB 공유를 결정할 때 다음 권장 사항을 염두에 두어야 합니다.

- BranchCache의 이점은 원격으로 캐시되는 데이터의 변경 사항이 자주 변경되는 경우 감소합니다.
- BranchCache 서비스는 여러 원격 사무소 클라이언트에서 다시 사용하거나 단일 원격 사용자가 반복적으로 액세스하는 파일 콘텐츠에 의해 다시 사용되는 파일 콘텐츠를 포함하는 공유에 유용합니다.



- 스냅샷 복사본 및 SnapMirror 대상에 있는 데이터와 같은 읽기 전용 콘텐츠에 대해 캐싱을 사용하도록 설정하는 것을 고려해 보십시오.

## BranchCache를 구성합니다

### BranchCache 개요를 구성합니다

ONTAP 명령을 사용하여 SMB 서버에서 BranchCache를 구성합니다. BranchCache를 구현하려면 클라이언트도 구성해야 하며, 콘텐츠를 캐시하려는 지사의 호스팅된 캐시 서버도 선택적으로 구성해야 합니다.

공유 단위로 캐싱을 사용하도록 BranchCache를 구성하는 경우 BranchCache 캐싱 서비스를 제공할 SMB 공유에서 BranchCache를 사용하도록 설정해야 합니다.

### BranchCache 구성 요구 사항

몇 가지 필수 구성 요소를 충족한 후 BranchCache를 설정할 수 있습니다.

SVM용 CIFS 서버에서 BranchCache를 구성하기 전에 다음 요구 사항이 충족되어야 합니다.

- ONTAP는 클러스터의 모든 노드에 설치해야 합니다.
- CIFS에 대한 라이선스가 있어야 하며 SMB 서버를 구성해야 합니다. SMB 라이선스는 에 포함되어 있습니다 ["ONTAP 1 을 참조하십시오"](#). ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.
- IPv4 또는 IPv6 네트워크 연결을 구성해야 합니다.
- BranchCache 1의 경우 SMB 2.1 이상이 활성화되어 있어야 합니다.
- BranchCache 2의 경우 SMB 3.0을 사용하도록 설정해야 하며 원격 Windows 클라이언트가 BranchCache 2를 지원해야 합니다.

### SMB 서버에서 BranchCache를 구성합니다

BranchCache를 구성하여 공유별로 BranchCache 서비스를 제공할 수 있습니다. 또는 BranchCache를 구성하여 모든 SMB 공유에서 캐싱을 자동으로 설정할 수 있습니다.

이 작업에 대해

SVM에서 BranchCache를 구성할 수 있습니다.

- CIFS 서버의 모든 SMB 공유 내에 포함된 모든 콘텐츠에 대해 캐싱 서비스를 제공하려는 경우 모든 공유 BranchCache 구성을 생성할 수 있습니다.
- CIFS 서버에서 선택한 SMB 공유 내에 포함된 콘텐츠에 대해 캐싱 서비스를 제공하려는 경우 공유당 BranchCache 구성을 생성할 수 있습니다.

BranchCache를 구성할 때는 다음 매개 변수를 지정해야 합니다.

필수 매개변수	설명
_SVM 이름 _	BranchCache는 SVM별로 구성됩니다. BranchCache 서비스를 구성할 CIFS 지원 SVM을 지정해야 합니다.

필수 매개변수	설명
해시 스토어에 대한 경로 _	<p>BranchCache 해시는 SVM 볼륨의 일반 파일에 저장됩니다. ONTAP에서 해시 데이터를 저장할 기존 디렉터리의 경로를 지정해야 합니다. BranchCache 해시 경로는 읽기/쓰기가 가능해야 합니다. 스냅샷 디렉토리나 같은 읽기 전용 경로는 허용되지 않습니다. 해시 데이터는 다른 데이터가 포함된 볼륨에 저장하거나 해시 데이터를 저장하기 위한 별도의 볼륨을 생성할 수 있습니다.</p> <p>SVM이 SVM 재해 복구 소스인 경우 해시 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨이 재해 복구 대상에 복제되지 않기 때문입니다.</p> <p>해시 경로에는 공백과 유효한 파일 이름 문자가 포함될 수 있습니다.</p>

필요에 따라 다음 매개 변수를 지정할 수 있습니다.

선택적 매개 변수입니다	설명
_지원되는 버전 _	ONTAP는 BranchCache 1 및 2를 지원합니다. 버전 1, 버전 2 또는 두 버전을 모두 사용할 수 있습니다. 기본값은 두 버전을 모두 사용하는 것입니다.
_해시 저장소의 최대 크기 _	해시 데이터 저장소에 사용할 크기를 지정할 수 있습니다. 해시 데이터가 이 값을 초과하면 ONTAP는 이전 해시를 삭제하여 새 해시를 위한 공간을 만듭니다. 해시 저장소의 기본 크기는 1GB입니다. BranchCache는 해시가 지나치게 공격적인 방식으로 폐기되지 않을 경우 보다 효율적으로 성능을 발휘합니다. 해시 저장소가 꽉 찼기 때문에 해시가 자주 삭제되는 경우 BranchCache 구성을 수정하여 해시 저장소 크기를 늘릴 수 있습니다.
_서버 키 _	BranchCache 서비스가 클라이언트가 BranchCache 서버를 가장하지 못하도록 하는 데 사용하는 서버 키를 지정할 수 있습니다. 서버 키를 지정하지 않으면 BranchCache 구성을 만들 때 서버 키가 임의로 생성됩니다. 여러 서버가 동일한 파일에 BranchCache 데이터를 제공하는 경우 클라이언트는 동일한 서버 키를 사용하는 모든 서버의 해시를 사용할 수 있도록 서버 키를 특정 값으로 설정할 수 있습니다. 서버 키에 공백이 있으면 서버 키를 따옴표로 묶어야 합니다.

선택적 매개 변수입니다	설명
_작동 모드_	<p>기본 설정은 공유별로 BranchCache를 사용하는 것입니다.</p> <ul style="list-style-type: none"> <li>• BranchCache 구성을 생성하여 공유별로 BranchCache를 사용하도록 설정하려면 이 선택적 매개 변수를 지정하지 않거나 "공유당"을 지정할 수 있습니다.</li> <li>• 모든 공유에서 BranchCache를 자동으로 활성화하려면 운영 모드를 '모든 공유'로 설정해야 합니다.</li> </ul>

## 단계

### 1. 필요에 따라 SMB 2.1 및 3.0 활성화:

- 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
- 구성된 SVM SMB 설정을 확인하여 필요한 모든 SMB 버전이 활성화되었는지 확인합니다. 'vserver cifs options show -vserver\_vserver\_name\_'
- 필요한 경우 SMB 2.1:'vserver cifs options modify -vserver\_vserver\_name\_-SMB2-enabled true'를 설정합니다

이 명령을 사용하면 SMB 2.0 및 SMB 2.1이 모두 설정됩니다.

- 필요한 경우 SMB 3.0:'vserver cifs options modify -vserver\_vserver\_name\_-SMB3-enabled true'를 설정합니다
- admin 권한 수준으로 복귀:'et-Privilege admin'입니다

### 2. BranchCache 구성:'vserver cifs BranchCache create-vserver\_name\_-hash-store-path path path [-hash-store-max-size{integer[KB|MB|GB|TB|PB]} [-versions{v1-enable|v2-enable|enable-all}][-server-key text] -operating-mode{per-share|all-share}]'

지정된 해시 스토리지 경로가 있어야 하며 SVM에서 관리하는 볼륨에 상주해야 합니다. 경로는 읽기 쓰기 가능 볼륨에도 있어야 합니다. 경로가 읽기 전용이거나 존재하지 않으면 명령이 실패합니다.

SVM BranchCache 구성을 추가할 때 동일한 서버 키를 사용하려면 서버 키에 대해 입력한 값을 기록합니다. BranchCache 구성에 대한 정보를 표시할 때는 서버 키가 나타나지 않습니다.

### 3. BranchCache 구성이 올바른지 확인합니다. 'vserver cifs BranchCache show -vserver\_vserver\_name\_'

## 예

다음 명령을 실행하면 SMB 2.1과 3.0이 모두 활성화되어 있고 SVM VS1의 모든 SMB 공유에서 캐싱이 자동으로 활성화되도록 BranchCache가 구성됩니다.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vservers cifs options show -vservers vs1 -fields smb2-
enabled,smb3-enabled
vservers smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vservers cifs branchcache create -vservers vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vservers cifs branchcache show -vservers vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: all_shares

```

다음 명령은 SMB 2.1과 3.0이 모두 활성화되어 있는지 확인하고, SVM VS1 기반 공유별로 캐싱이 가능하도록 BranchCache를 구성하고, BranchCache 구성을 확인합니다.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share

```

## 관련 정보

[요구 사항 및 지침: BranchCache 버전 지원](#)

[원격 사무소에서 BranchCache 구성에 대한 정보를 찾을 수 있는 위치](#)

[BranchCache 지원 SMB 공유를 생성합니다](#)

[기존 SMB 공유에서 BranchCache를 사용하도록 설정합니다](#)

[BranchCache 구성을 수정합니다](#)

[SMB 공유에서 BranchCache를 해제합니다. 개요](#)

[SVM에서 BranchCache 구성을 삭제합니다](#)

원격 사무소에서 **BranchCache** 구성에 대한 정보를 찾을 수 있는 위치

SMB 서버에서 BranchCache를 구성한 후에는 클라이언트 컴퓨터에 BranchCache를 설치하고 구성해야 하며, 필요에 따라 원격 사무실의 캐싱 서버에 BranchCache를 설치하고 구성해야 합니다. Microsoft는 원격 사무소에서 BranchCache를 구성하는 지침을 제공합니다.

지점 클라이언트 구성 지침 및 BranchCache를 사용할 캐싱 서버(선택 사항)는 Microsoft BranchCache 웹 사이트에 있습니다.

## "Microsoft BranchCache 문서: 새로운 기능"

### BranchCache 지원 SMB 공유를 구성합니다

#### BranchCache 지원 SMB 공유 구성 개요

SMB 서버 및 지사에 BranchCache를 구성한 후에는 지점의 클라이언트가 캐시할 콘텐츠를 포함하는 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

BranchCache 캐싱은 SMB 서버의 모든 SMB 공유 또는 공유별로 설정할 수 있습니다.

- 공유별로 BranchCache를 사용하도록 설정한 경우 공유를 생성하거나 기존 공유를 수정하여 BranchCache를 사용하도록 설정할 수 있습니다.

기존 SMB 공유에서 캐싱을 사용하는 경우 ONTAP는 해당 공유에서 BranchCache를 사용하도록 설정하는 즉시 해시 컴퓨팅을 시작하고 콘텐츠를 요청하는 클라이언트로 메타데이터를 전송합니다.

- 이전에 SMB로 공유에 접속한 클라이언트는 이후에 BranchCache가 해당 공유에 설정된 경우 BranchCache 지원을 받지 못합니다.

ONTAP는 SMB 세션이 설정된 시간에 공유에 대한 BranchCache 지원을 알립니다. BranchCache를 사용하도록 설정할 때 이미 세션을 설정한 클라이언트는 연결을 끊고 다시 연결하여 이 공유에 캐시된 콘텐츠를 사용해야 합니다.



이후에 SMB 공유의 BranchCache가 비활성화되면 ONTAP는 요청 클라이언트로 메타데이터 전송을 중지합니다. 데이터가 필요한 클라이언트는 콘텐츠 서버(SMB 서버)에서 직접 검색합니다.

#### BranchCache 지원 SMB 공유를 생성합니다

공유를 생성할 때 "BranchCache" 공유 속성을 설정하여 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SMB 공유에 BranchCache가 설정되어 있으면 공유에 수동 캐싱으로 설정된 오프라인 파일 구성이 있어야 합니다.

공유를 생성할 때 기본 설정입니다.

- BranchCache 사용 공유를 생성할 때 추가 선택적 공유 매개 변수를 지정할 수도 있습니다.
- BranchCache가 SVM(스토리지 가상 시스템)에서 구성 및 설정되지 않은 경우에도 공유에 "BranchCache" 속성을 설정할 수 있습니다.

그러나 공유 폴더에 캐시된 콘텐츠가 제공되도록 하려면 SVM에서 BranchCache를 구성하고 사용하도록 설정해야 합니다.

- '-share-properties' 매개 변수를 사용할 때 공유에 적용되는 기본 공유 속성이 없으므로 쉼표로 구분된 목록을 사용하여 "BranchCache" 공유 속성 외에도 공유에 적용할 다른 모든 공유 속성을 지정해야 합니다.
- 자세한 내용은 'vserver cifs share create' 명령에 대한 man 페이지를 참조하십시오.

## 단계

1. BranchCache 지원 SMB 공유 생성: + 'vserver CIFS share create -vserver \_vserver\_name\_ -share -name \_share\_name\_ -path \_path\_ -share-properties BranchCache[,...]'
2. 'vserver cifs share show' 명령을 사용하여 SMB 공유에 BranchCache 공유 속성이 설정되어 있는지 확인합니다.

## 예

다음 명령을 실행하면 SVM VS1 에서 "/data " 경로를 사용하여 " data " 라는 BranchCache 지원 SMB 공유가 생성됩니다. 기본적으로 오프라인 파일 설정은 '수동'으로 설정됩니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
      Vserver: vs1
      Share: data
CIFS Server NetBIOS Name: VS1
      Path: /data
      Share Properties: branchcache
                       oplocks
                       browsable
                       changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

## 관련 정보

[단일 SMB 공유에서 BranchCache를 사용하지 않도록 설정합니다](#)

기존 **SMB** 공유에서 **BranchCache**를 사용하도록 설정합니다

기존 공유 속성 목록에 'BranchCache' 공유 속성을 추가하여 기존 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

## 이 작업에 대해

- SMB 공유에 BranchCache가 설정되어 있으면 공유에 수동 캐싱으로 설정된 오프라인 파일 구성이 있어야 합니다.

기존 공유의 오프라인 파일 설정이 수동 캐싱으로 설정되어 있지 않으면 공유를 수정하여 구성해야 합니다.

- BranchCache가 SVM(스토리지 가상 시스템)에서 구성 및 설정되지 않은 경우에도 공유에 "BranchCache" 속성을 설정할 수 있습니다.

그러나 공유 폴더에 캐시된 콘텐츠가 제공되도록 하려면 SVM에서 BranchCache를 구성하고 사용하도록 설정해야 합니다.

- 공유에 "BranchCache" 공유 속성을 추가하면 기존 공유 설정과 공유 속성이 유지됩니다.

BranchCache 공유 속성이 기존 공유 속성 목록에 추가됩니다. 'vserver cifs share properties add' 명령 사용에 대한 자세한 내용은 man 페이지를 참조하십시오.

#### 단계

1. 필요한 경우 수동 캐싱에 대한 오프라인 파일 공유 설정을 구성합니다.
  - a. 'vserver cifs share show' 명령을 사용하여 오프라인 파일 공유 설정을 확인합니다.
  - b. 오프라인 파일 공유 설정이 manual로 설정되어 있지 않으면 필요한 값('vserver cifs share modify -vserver vserver\_name -share-name share\_name -offline-files manual')으로 변경합니다
2. 기존 SMB 공유에서 BranchCache를 사용하도록 설정합니다. 'vserver cifs share properties add-vserver vserver\_name -share-name share\_name-share-properties BranchCache'
3. SMB 공유에서 BranchCache 공유 속성이 설정되어 있는지 확인합니다. 'vserver cifs share show -vserver vserver\_name -share-name share\_name'

#### 예

다음 명령을 실행하면 SVM VS1 에서 " data2 " 라는 기존 SMB 공유에서 "/data2 " 경로를 사용하여 BranchCache를 사용할 수 있습니다.



```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data2
```

```

    Vserver: vs1
    Share: data2
    CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vsserver cifs share properties add -vsserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data2
```

```

    Vserver: vs1
    Share: data2
    CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     showsnapshot
                     changenotify
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

## BranchCache 구성을 관리하고 모니터링합니다

### BranchCache 구성을 수정합니다

해시 저장소 디렉토리 경로 변경, 해시 저장소 최대 디렉토리 크기, 운영 모드 및 지원되는 BranchCache 버전을 포함하여 SVM에서 BranchCache 서비스의 구성을 수정할 수 있습니다. 해시 저장소가 포함된 볼륨의 크기를 늘릴 수도 있습니다.

#### 단계

1. 적절한 작업을 수행합니다.

원하는 작업	다음을 입력하십시오.
해시 저장소 디렉터리 크기를 수정합니다	'vserver cifs BranchCache modify -vserver vservice_name -hash-store -max-size{integer[KB
MB	GB
TB	PB]]'
해시 저장소가 포함된 볼륨의 크기를 늘립니다	``볼륨 크기 - vservice vservice_name - volume volume_name - new-size new_size [k
m	g
t]` 해시 저장소가 포함된 볼륨이 가득 차면 볼륨의 크기를 늘릴 수 있습니다. 새 볼륨 크기를 숫자로 지정한 다음 단위를 지정할 수 있습니다.	해시 저장소 디렉터리 경로를 수정합니다
에 대해 자세히 알아보십시오 " <a href="#">FlexVol 볼륨 관리</a> "	
'vserver cifs BranchCache modify -vserver vservice_name -hash-store-path path -flush -hash{true	<p>false}' SVM이 SVM 재해 복구 소스인 경우 해시 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨이 재해 복구 대상에 복제되지 않기 때문입니다.</p> <p>BranchCache 해시 경로에는 공백과 유효한 파일 이름 문자가 포함될 수 있습니다.</p> <p>해시 경로를 수정할 경우 ONTAP가 원래 해시 저장 위치에서 해시를 플러시할지 여부를 지정하는 필수 매개 변수입니다. '-flush-hash' 파라미터에 대해 다음 값을 설정할 수 있습니다.</p> <p><b>"true"</b>를 지정하면 <b>ONTAP</b>는 원래 위치에서 해시를 삭제하고 <b>BranchCache</b> 사용 클라이언트가 새 요청을 수행할 때 새 위치에 새 해시를 만듭니다. <b>false</b>를 지정하면 해시가 플러시되지 않습니다. + 이 경우 해시 저장소 경로를 원래 위치로 다시 변경하여 나중에 기존 해시를 다시 사용하도록 선택할 수 있습니다.</p>

원하는 작업	다음을 입력하십시오.
작동 모드를 변경합니다	'vserver cifs BranchCache modify -vserver vserver_name -operating-mode{per-share
all-share	disable}'  작동 모드를 수정할 때 다음 사항에 유의해야 합니다.  <b>ONTAP</b> 는 <b>SMB</b> 세션이 설정되어 있을 때 공유에 대한 <b>BranchCache</b> 지원을 알립니다. BranchCache를 사용하도록 설정할 때 이미 세션을 설정한 클라이언트는 연결을 끊고 다시 연결하여 이 공유에 캐시된 콘텐츠를 사용해야 합니다.
BranchCache 버전 지원을 변경합니다	'vserver cifs BranchCache modify -vserver vserver_name -versions{v1-enable
v2-enable	enable-all}'

2. 'vserver cifs BranchCache show' 명령을 사용하여 구성 변경 사항을 확인합니다.

**BranchCache** 구성에 대한 정보를 표시합니다

구성을 확인하거나 구성을 수정하기 전에 현재 설정을 확인할 때 사용할 수 있는 SVM(스토리지 가상 머신)에 BranchCache 구성에 대한 정보를 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

를 표시하려면...	이 명령을 입력하십시오...
모든 SVM의 BranchCache 구성에 대한 요약 정보	'vserver cifs BranchCache show'를 선택합니다
특정 SVM의 구성에 대한 자세한 정보	'vserver cifs BranchCache show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 BranchCache 구성에 대한 정보를 표시합니다.

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

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

**BranchCache** 서버 키를 변경합니다

SVM(스토리지 가상 시스템)에서 BranchCache 구성을 수정하고 다른 서버 키를 지정하여 BranchCache 서버 키를 변경할 수 있습니다.

이 작업에 대해

여러 서버가 동일한 파일에 BranchCache 데이터를 제공하는 경우 클라이언트는 동일한 서버 키를 사용하는 모든 서버의 해시를 사용할 수 있도록 서버 키를 특정 값으로 설정할 수 있습니다.

서버 키를 변경할 때는 해시 캐시도 플러시해야 합니다. 해시를 플러싱한 후 ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

단계

1. 'vserver cifs BranchCache modify -vserver vserver\_name -server-key text -flush -hash true' 명령을 사용하여 서버 키를 변경합니다

새 서버 키를 구성할 때는 -flush-hash를 지정하고 값을 true로 설정해야 합니다.

2. 'vserver cifs BranchCache show' 명령을 사용하여 BranchCache 구성이 올바른지 확인합니다.

예

다음 예에서는 공백이 포함된 새 서버 키를 설정하고 SVM VS1의 해시 캐시를 플러시합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

관련 정보

## ONTAP가 BranchCache 해시를 무효화하는 이유

지정된 경로에 대한 **BranchCache** 해시 사전 계산

BranchCache 서비스를 구성하여 단일 파일, 디렉토리 또는 디렉토리 구조의 모든 파일에 대한 해시를 사전 계산할 수 있습니다. 이 방법은 사용량이 많지 않은 시간 동안 BranchCache 사용 공유의 데이터에 대한 해시를 계산할 때 유용합니다.

이 작업에 대해

해시 통계를 표시하기 전에 데이터 샘플을 수집하려면 '통계 시작' 및 '통계 중지' 옵션 명령을 사용해야 합니다.

- 사전 컴퓨팅 해시를 계산할 스토리지 가상 시스템(SVM)과 경로를 지정해야 합니다.
- 또한 해시를 재귀적으로 계산할 것인지 여부를 지정해야 합니다.
- 해시를 재귀적으로 계산하려는 경우 BranchCache 서비스는 지정된 경로 아래의 전체 디렉토리 트리를 탐색한 다음 각 대상 객체에 대한 해시를 계산합니다.

단계

1. 원하는 대로 사전 계산 해시:

에서 해시를 사전 계산하려는 경우...	명령 입력...
단일 파일 또는 디렉토리입니다	'vserver cifs BranchCache hash-create-vserver vserver_name-path path-recurse false'
디렉토리 구조의 모든 파일에 반복적으로 존재합니다	'vserver cifs BranchCache hash-create-vserver vserver_name-path absolute_path-recurse true'

2. '통계' 명령을 사용하여 해시가 계산되는지 확인합니다.

- 원하는 SVM 인스턴스에 대한 'hashd' 객체 통계 표시: 'statistics show-object hashd-instance  
vserver\_name'
- 명령을 반복하여 생성된 해시 수가 증가하는지 확인합니다.

예

다음 예에서는 경로 '/data'와 SVM VS1의 모든 포함된 파일 및 하위 디렉토리에 해시를 생성합니다.

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

관련 정보

["성능 모니터링 설정"](#)

**SVM BranchCache** 해시 저장소에서 해시를 플러시합니다

SVM(스토리지 가상 머신)의 BranchCache 해시 저장소에서 캐시된 모든 해시를 플러시할 수 있습니다. 지사 BranchCache 구성을 변경한 경우 이 기능이 유용할 수 있습니다. 예를 들어 최근에 분산 캐싱에서 호스팅된 캐싱 모드로 캐싱 모드를 재구성한 경우 해시 저장소를 플러시해야 합니다.

이 작업에 대해

해시를 플러싱한 후 ONTAP은 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

단계

1. BranchCache 해시 저장소에서 해시를 플러시합니다. 'vserver cifs BranchCache hash-flush-vserver\_vserver\_name\_'

```
'vserver cifs BranchCache hash-flush-vserver vs1'
```

**BranchCache** 통계를 표시합니다

BranchCache 통계를 에 표시할 수도 있습니다. 그 중에서도 캐싱을 얼마나 잘 수행하고 있는지 식별하고, 구성이 클라이언트에 캐시된 콘텐츠를 제공하고 있는지 여부를 확인하고, 해시 파일을 삭제하여 최신 해시 데이터를 저장할 공간을 확보할 수 있는지 확인할 수 있습니다.

이 작업에 대해

"hashd" 통계 객체에는 BranchCache 해시에 대한 통계 정보를 제공하는 카운터가 포함되어 있습니다. CIFS 통계 객체에는 BranchCache 관련 작업에 대한 통계 정보를 제공하는 카운터가 포함되어 있습니다. 고급 권한 수준에서 이러한 개체에 대한 정보를 수집하고 표시할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. 'istics catalog counter show' 명령을 사용하여 BranchCache 관련 카운터를 출력한다.

통계 카운터에 대한 자세한 내용은 이 명령의 man 페이지를 참조하십시오.

```
cluster1::*> statistics catalog counter show -object hashd
```

```
Object: hashd
```

Counter	Description
-----	-----
-----	-----

branchcache_hash_created	Number of times a request to generate BranchCache hash for a file succeeded.
branchcache_hash_files_replaced	Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
branchcache_hash_rejected	Number of times a request to generate BranchCache hash data failed.
branchcache_hash_store_bytes	Total number of bytes used to store hash data.
branchcache_hash_store_size	Total space used to store BranchCache hash data for the Vserver.
instance_name	Instance Name
instance_uuid	Instance UUID
node_name	System node name
node_uuid	System node id

9 entries were displayed.

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
-----	-----
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail	Total number of times a request to fetch hash data failed. These are failures when attempting to read existing hash data. It does not include attempts to fetch hash



```

data
                                that has not yet been generated.
    branchcache_hash_fetch_ok    Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes  Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
....Output truncated....

```

3. '스타티틱스 스타트', '스타티틱스 스톱' 명령어를 사용해 BranchCache 관련 통계를 수집한다.

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. 통계 표시 명령을 사용하여 수집된 BranchCache 통계를 표시합니다.

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

##### 5. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

```
cluster1::*> set -privilege admin
```

관련 정보

[통계를 표시합니다](#)

["성능 모니터링 설정"](#)

**BranchCache** 그룹 정책 개체 지원

ONTAP BranchCache는 특정 BranchCache 구성 매개 변수에 대한 중앙 집중식 관리를

허용하는 BranchCache GPO(그룹 정책 개체)를 지원합니다. BranchCache에는 두 가지 GPO, 즉 BranchCache GPO의 해시 게시 GPO와 BranchCache GPO의 해시 버전 지원 GPO가 사용됩니다.

- \* BranchCache GPO \* 용 해시 게시

BranchCache GPO의 해시 게시는 '-operating-mode' 매개 변수에 해당합니다. GPO 업데이트가 발생하면 이 값은 그룹 정책이 적용되는 OU(조직 구성 단위) 내에 포함된 SVM(스토리지 가상 시스템) 개체에 적용됩니다.

- \* BranchCache GPO \* 에 대한 해시 버전 지원

BranchCache GPO의 해시 버전 지원은 '-versions' 매개 변수에 해당합니다. GPO 업데이트가 발생하면 이 값은 그룹 정책이 적용되는 조직 구성 단위 내에 포함된 SVM 개체에 적용됩니다.

## 관련 정보

### CIFS 서버에 그룹 정책 객체 적용

**BranchCache** 그룹 정책 개체에 대한 정보를 표시합니다

CIFS 서버의 GPO(그룹 정책 개체) 구성에 대한 정보를 표시하여 BranchCache GPO가 CIFS 서버가 속한 도메인에 대해 정의되었는지 그리고 그러한 경우 허용되는 설정이 무엇인지 확인할 수 있습니다. 또한 BranchCache GPO 설정이 CIFS 서버에 적용되는지 여부를 확인할 수 있습니다.

## 이 작업에 대해

CIFS 서버가 속한 도메인 내에서 GPO 설정이 정의되더라도 CIFS 지원 SVM(스토리지 가상 머신)이 포함된 OU(조직 구성 단위)에는 적용되지 않을 수도 있습니다. 적용된 GPO 설정은 CIFS 지원 SVM에 적용되는 정의된 모든 GPO의 하위 집합입니다. GPO를 통해 적용된 BranchCache 설정은 CLI를 통해 적용된 설정을 재정의합니다.

## 단계

1. 'vserver cifs group-policy show-defined' 명령을 사용하여 Active Directory 도메인에 대해 정의된 BranchCache GPO 설정을 표시합니다.



이 예제에는 명령에 사용할 수 있는 출력 필드가 모두 표시되지 않습니다. 출력이 잘립니다.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication for Mode BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

2. 'vserver cifs group-policy show-applied' 명령을 사용하여 CIFS 서버에 적용된 BranchCache GPO 설정을 표시합니다. ``이



이 예제에는 명령에 사용할 수 있는 출력 필드가 모두 표시되지 않습니다. 출력이 잘립니다.

```
cluster1::> vsriver cifs group-policy show-applied -vsriver vs1

Vserver: vs1
-----
    GPO Name: Default Domain Policy
      Level: Domain
      Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]

    GPO Name: Resultant Set of Policy
      Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]
```

## 관련 정보

[CIFS 서버에서 GPO 지원을 설정하거나 해제합니다](#)

**SMB** 공유에서 **BranchCache**를 해제합니다

**SMB** 공유에서 **BranchCache**를 해제합니다. 개요

특정 SMB 공유에서 BranchCache 캐싱 서비스를 제공하지 않고 나중에 이러한 공유에 캐싱 서비스를 제공하려는 경우 공유별로 BranchCache를 사용하지 않도록 설정할 수 있습니다. BranchCache가 모든 공유에서 캐싱을 제공하도록 구성되었지만 모든 캐싱 서비스를 일시적으로 해제하려면 BranchCache 구성을 수정하여 모든 공유에서 자동 캐싱을 중지할 수 있습니다.

SMB 공유의 BranchCache가 이후에 처음 설정된 후 비활성화되면 ONTAP은 요청된 클라이언트로 메타데이터 전송을 중지합니다. 데이터가 필요한 클라이언트는 콘텐츠 서버(SVM(Storage Virtual Machine)의 CIFS 서버)에서 직접 데이터를 검색합니다.

## 관련 정보

### BranchCache 지원 SMB 공유 구성

단일 **SMB** 공유에서 **BranchCache**를 비활성화합니다

이전에 캐시된 콘텐츠를 제공한 특정 공유에 캐싱 서비스를 제공하지 않으려면 기존 SMB 공유에서 BranchCache를 사용하지 않도록 설정할 수 있습니다.

#### 단계

1. 'vserver cifs share properties remove-vserver vserver\_name -share-name share\_name-share-properties BranchCache' 명령을 입력합니다

BranchCache 공유 속성이 제거됩니다. 다른 적용된 공유 속성은 그대로 유지됩니다.

#### 예

다음 명령을 실행하면 이름이 "data2"인 기존 SMB 공유에서 BranchCache가 비활성화됩니다.

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties remove -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

모든 **SMB** 공유에서 자동 캐싱을 중지합니다

BranchCache 구성에서 각 SVM(스토리지 가상 머신)의 모든 SMB 공유에 대한 캐싱을 자동으로 설정하는 경우 BranchCache 구성을 수정하여 모든 SMB 공유의 콘텐츠를 자동으로 캐싱하지 않도록 할 수 있습니다.

이 작업에 대해

모든 SMB 공유에서 자동 캐싱을 중지하려면 BranchCache 운영 모드를 공유 기준 캐싱으로 변경합니다.

단계

1. 모든 SMB 공유에서 자동 캐싱을 중지하도록 BranchCache를 구성합니다. 'vserver cifs BranchCache modify -vserver vs1 -operating-mode per-share'
2. BranchCache 구성이 올바른지 확인합니다. 'vserver cifs BranchCache show -vserver vs1'

예

다음 명령을 실행하면 스토리지 가상 머신(SVM, 이전의 Vserver)의 BranchCache 구성이 변경되어 모든 SMB 공유에서 자동 캐싱을 중지합니다.

```
cluster1::> vs1 cifs branchcache modify -vserver vs1 -operating-mode per-share

cluster1::> vs1 cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

**SVM에서 BranchCache를 비활성화하거나 활성화합니다**

**CIFS** 서버에서 **BranchCache**를 해제하거나 다시 설정하면 어떻게 됩니까

이전에 BranchCache를 구성했지만 지사 클라이언트가 캐시된 콘텐츠를 사용하지 않도록 하려면 CIFS 서버에서 캐싱을 해제할 수 있습니다. BranchCache를 사용하지 않도록 설정하면 어떤 일이 발생하는지 알고 있어야 합니다.

BranchCache를 사용하지 않도록 설정하면 ONTAP는 더 이상 해시를 계산하지 않고 요청 클라이언트로 메타데이터를 보내지 않습니다. 그러나 파일 액세스는 중단되지 않습니다. 그 후 BranchCache를 사용하는 클라이언트가 액세스할 콘텐츠에 대한 메타데이터 정보를 요청하면 ONTAP는 Microsoft 정의 오류로 응답하여 클라이언트가 실제 콘텐츠를 요청하는 두 번째 요청을 보냅니다. CIFS 서버는 콘텐츠 요청에 따라 SVM(스토리지 가상 머신)에 저장된 실제 콘텐츠를 전송합니다.

CIFS 서버에서 BranchCache를 사용하지 않도록 설정한 후 SMB 공유는 BranchCache 기능을 알리지 않습니다. 새 SMB 연결에서 데이터에 액세스하기 위해 클라이언트는 SMB 읽기 요청을 정상적으로 처리합니다.



언제든지 CIFS 서버에서 BranchCache를 다시 설정할 수 있습니다.

- BranchCache를 비활성화하면 해시 저장소가 삭제되지 않으므로 요청된 해시가 여전히 유효하다면 ONTAP는 해시 요청을 다시 활성화한 후 해시 요청에 응답할 때 저장된 해시를 사용할 수 있습니다.
- BranchCache를 사용하지 않는 동안 BranchCache 사용 공유에 SMB 연결을 설정한 클라이언트는 BranchCache를 나중에 다시 사용하도록 설정한 경우 BranchCache 지원을 받지 않습니다.

이는 ONTAP가 SMB 세션을 설정할 때 공유에 대한 BranchCache 지원을 광고하기 때문입니다. BranchCache를 사용하지 않는 동안 BranchCache 사용 공유에 세션을 설정한 클라이언트는 이 공유에 대해 캐시된 콘텐츠를 사용하려면 연결을 끊고 다시 연결해야 합니다.



CIFS 서버에서 BranchCache를 해제한 후에 해시 저장소를 저장하지 않으려면 수동으로 삭제할 수 있습니다. BranchCache를 다시 사용하도록 설정하는 경우 해시 저장소 디렉터리가 있는지 확인해야 합니다. BranchCache를 다시 사용하도록 설정한 후 BranchCache 사용 공유는 BranchCache 기능을 광고합니다. ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

**BranchCache**를 비활성화하거나 활성화합니다

BranchCache 운영 모드를 사용 안 함으로 변경하여 SVM(스토리지 가상 시스템)에서 BranchCache를 사용하지 않도록 설정할 수 있습니다. 운영 모드를 변경하여 BranchCache 서비스를 공유당 제공하거나 모든 공유에 자동으로 제공하여 언제든지 BranchCache를 활성화할 수 있습니다.

단계

1. 적절한 명령을 실행합니다.

원하는 작업	그런 다음 다음을 입력합니다.
BranchCache를 비활성화합니다	'vserver cifs BranchCache modify -vserver vservice_name -operating-mode disable'
공유당 BranchCache를 설정합니다	'vserver cifs BranchCache modify -vserver vservice_name -operating-mode per-share'
모든 공유에 대해 BranchCache를 사용하도록 설정합니다	'vserver cifs BranchCache modify -vserver vservice_name -operating-mode all-공유'

2. BranchCache 작동 모드가 'vserver cifs BranchCache show -vserver vservice\_name' 설정으로 구성되어 있는지 확인합니다

예

다음 예에서는 SVM VS1 에서 BranchCache를 사용하지 않도록 설정합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable
```

## SVM에서 BranchCache 구성을 삭제합니다

BranchCache 구성을 삭제하면 어떻게 됩니까

이전에 BranchCache를 구성했지만 SVM(스토리지 가상 시스템)이 캐시된 콘텐츠를 계속 제공하지 않도록 하려면 CIFS 서버에서 BranchCache 구성을 삭제할 수 있습니다. 구성을 삭제할 때 어떤 일이 발생하는지 알고 있어야 합니다.

구성을 삭제하면 ONTAP에서 해당 SVM에 대한 구성 정보를 클러스터에서 제거하고 BranchCache 서비스를 중지합니다. ONTAP에서 SVM의 해시 저장소를 삭제할 것인지 여부를 선택할 수 있습니다.

BranchCache 구성을 삭제해도 BranchCache 사용 클라이언트의 액세스가 중단되지 않습니다. 그 후 BranchCache를 사용하는 클라이언트가 이미 캐시된 콘텐츠에 대한 기존 SMB 연결에 대한 메타데이터 정보를 요청하면 ONTAP는 Microsoft 정의 오류로 응답하여 클라이언트가 실제 콘텐츠를 요청하는 두 번째 요청을 보냅니다. CIFS 서버는 콘텐츠 요청에 응답하여 SVM에 저장된 실제 콘텐츠를 전송합니다

BranchCache 구성이 삭제된 후 SMB 공유는 BranchCache 기능을 알리지 않습니다. 새 SMB 연결을 사용하여 이전에 캐시되지 않은 콘텐츠에 액세스하려면 클라이언트는 SMB 읽기 요청을 정상적으로 처리합니다.

BranchCache 구성을 삭제합니다

SVM(스토리지 가상 시스템)에서 BranchCache 서비스를 삭제하는 데 사용하는 명령은 기존 해시를 삭제하거나 유지할지 여부에 따라 달라집니다.

단계

1. 적절한 명령을 실행합니다.

원하는 작업	그런 다음 다음을 입력합니다.
BranchCache 구성을 삭제하고 기존 해시를 삭제합니다	'vserver cifs BranchCache delete -vserver_vserver_name_-flush-hash true
BranchCache 구성을 삭제하지만 기존 해시는 그대로 둡니다	'vserver cifs BranchCache delete -vserver_vserver_name_-flush-hash false

예

다음 예에서는 SVM VS1 상의 BranchCache 구성을 삭제하고 기존 해시를 모두 삭제합니다.

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes true
```

되돌릴 때 **BranchCache**가 어떻게 됩니까

ONTAP을 BranchCache를 지원하지 않는 릴리즈로 되돌릴 경우 어떤 일이 발생하는지 이해하는 것이 중요합니다.

- BranchCache를 지원하지 않는 ONTAP 버전으로 되돌릴 경우 SMB 공유는 BranchCache를 사용하는 클라이언트에 BranchCache 기능을 알리지 않으므로 클라이언트는 해시 정보를 요청하지 않습니다.

대신 일반 SMB 읽기 요청을 사용하여 실제 콘텐츠를 요청합니다. 콘텐츠 요청에 따라 SMB 서버는 SVM(스토리지 가상 머신)에 저장된 실제 콘텐츠를 전송합니다.

- 해시 저장소를 호스팅하는 노드가 BranchCache를 지원하지 않는 릴리즈로 되돌려지면 스토리지 관리자는 복원 중에 인쇄되는 명령을 사용하여 BranchCache 구성을 수동으로 되돌려야 합니다.

이 명령을 실행하면 BranchCache 구성 및 해시가 삭제됩니다.

복원이 완료된 후 스토리지 관리자는 원하는 경우 해시 저장소가 포함된 디렉토리를 수동으로 삭제할 수 있습니다.

관련 정보

[SVM에서 BranchCache 구성을 삭제합니다](#)

## Microsoft 원격 복제 성능 향상

### Microsoft 원격 복제 성능 개요 개선

Microsoft ODX(Offloaded Data Transfer)는 `_copy offload_`라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고도 호환되는 스토리지 장치 내부 또는 간에 데이터를 직접 전송할 수 있습니다.

ONTAP은 SMB 및 SAN 프로토콜을 모두 지원하는 ODX를 지원합니다. 소스는 CIFS 서버 또는 LUN일 수 있으며 대상은 CIFS 서버 또는 LUN일 수 있습니다.

ODX가 아닌 파일을 전송하면 소스에서 데이터를 읽어 네트워크를 통해 클라이언트 컴퓨터로 전송합니다. 클라이언트 컴퓨터는 네트워크를 통해 데이터를 대상으로 다시 전송합니다. 요약하면 클라이언트 컴퓨터는 소스에서 데이터를 읽고 대상에 씁니다. ODX 파일 전송을 사용하면 데이터가 소스에서 타겟으로 직접 복사됩니다.

오프로드 복사본은 소스 및 타겟 스토리지 간에 직접 수행되므로 성능이 크게 향상됩니다. 소스 및 대상 간의 복제 시간 단축, 클라이언트의 리소스 활용률(CPU, 메모리) 감소, 네트워크 I/O 대역폭 사용률 감소 등의 성능 이점을 얻을 수 있습니다.

SMB 환경의 경우 이 기능은 클라이언트와 스토리지 서버가 모두 SMB 3.0 및 ODX 기능을 지원하는 경우에만 사용할 수 있습니다. SAN 환경의 경우 이 기능은 클라이언트와 스토리지 서버가 ODX 기능을 모두 지원하는 경우에만 사용할 수 있습니다. ODX를 지원하고 ODX를 사용하는 클라이언트 컴퓨터는 파일을 이동하거나 복사할 때 오프로드된 파일

전송을 자동으로 투명하게 사용합니다. ODX는 Windows 탐색기를 통해 파일을 끌어서 놓을지, 명령줄 파일 복사 명령을 사용하는지, 클라이언트 애플리케이션이 파일 복사 요청을 시작하는지 여부와 관계없이 사용됩니다.

#### 관련 정보

자동 위치를 사용하여 SMB 자동 노드 조회를 제공하여 클라이언트 응답 시간을 단축합니다

"Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"

#### ODX의 작동 방식

ODX 복사 오프로드는 토큰 기반 메커니즘을 사용하여 ODX 지원 CIFS 서버 내부 또는 간에 데이터를 읽고 씁니다. CIFS 서버는 데이터를 호스트를 통해 라우팅하는 대신 데이터를 나타내는 작은 토큰을 클라이언트에 보냅니다. ODX 클라이언트는 해당 토큰을 대상 서버에 제공하고, 이 토큰을 통해 표시되는 데이터를 소스에서 타겟으로 전송할 수 있습니다.

ODX 클라이언트는 CIFS 서버가 ODX를 지원하는 서버임을 인식하면 소스 파일을 열고 CIFS 서버에서 토큰을 요청합니다. 대상 파일을 연 후 클라이언트는 토큰을 사용하여 서버에서 데이터를 소스에서 대상으로 직접 복사하도록 지시합니다.

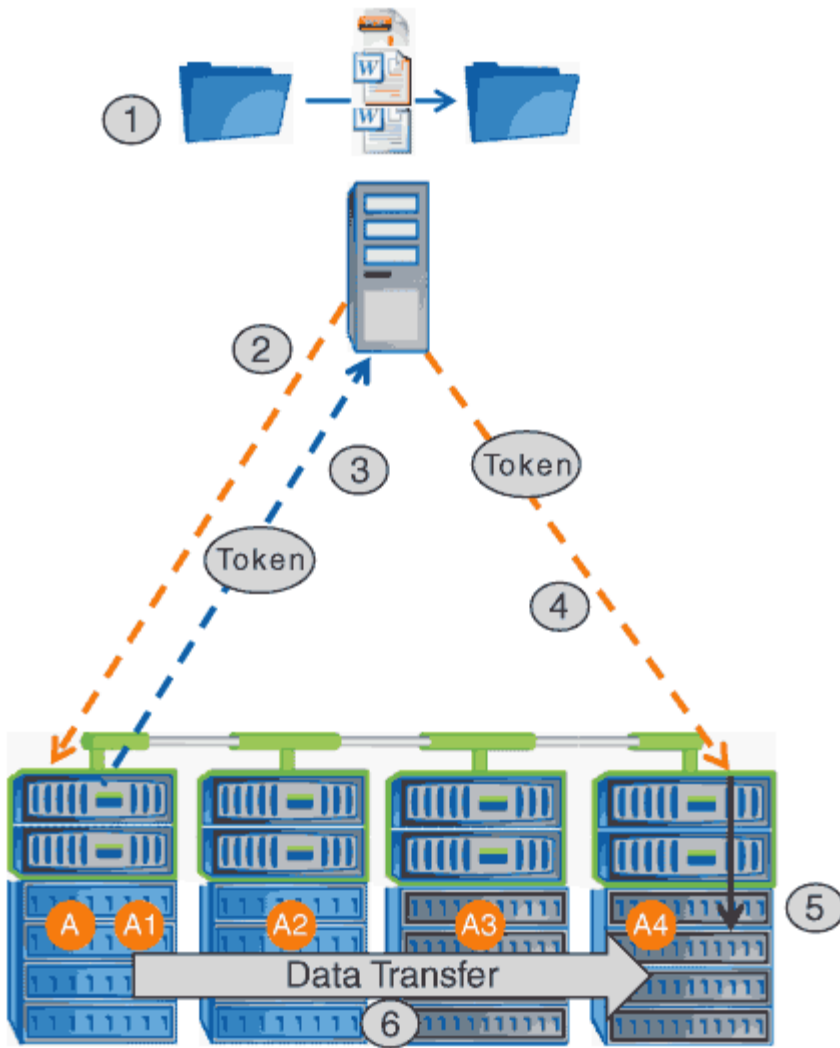


복사 작업의 범위에 따라 소스 및 대상이 동일한 SVM(스토리지 가상 머신) 또는 다른 SVM에 있을 수 있습니다.

토큰은 데이터의 시점 표현의 역할을 합니다. 예를 들어, 스토리지 위치 간에 데이터를 복사할 때 데이터 세그먼트를 나타내는 토큰이 요청 클라이언트로 반환되고, 이 클라이언트는 대상에 복사되므로 클라이언트를 통해 기본 데이터를 복사할 필요가 없습니다.

ONTAP는 8MB의 데이터를 나타내는 토큰을 지원합니다. 8MB를 초과하는 ODX 복제본은 8MB의 데이터를 나타내는 각 토큰과 함께 여러 토큰을 사용하여 수행됩니다.

다음 그림에서는 ODX 복사 작업과 관련된 단계를 설명합니다.



1. 사용자가 Windows 탐색기, 명령줄 인터페이스 또는 가상 시스템 마이그레이션의 일부로 파일을 복사 또는 이동하거나 응용 프로그램이 파일 복사 또는 이동을 시작합니다.
2. ODX 지원 클라이언트는 이 전송 요청을 ODX 요청으로 자동 변환합니다.

CIFS 서버로 전송되는 ODX 요청에 토큰에 대한 요청이 있습니다.

3. CIFS 서버에서 ODX가 설정되어 있고 연결이 SMB 3.0을 통해 설정되어 있으면 CIFS 서버가 토큰을 생성합니다. 이는 소스에서 데이터를 논리적으로 표현한 것입니다.
4. 클라이언트는 데이터를 나타내는 토큰을 받아 쓰기 요청과 함께 대상 CIFS 서버로 전송합니다.

이 데이터는 네트워크를 통해 소스에서 클라이언트로 복사한 다음 클라이언트에서 대상으로 복사하는 유일한 데이터입니다.

5. 토큰이 스토리지 서브시스템에 제공됩니다.
6. SVM은 내부적으로 복사 또는 이동을 수행합니다.

복사 또는 이동된 파일이 8MB보다 큰 경우 복제를 수행하려면 여러 토큰이 필요합니다. 필요에 따라 복사를 완료하기 위해 2-6단계를 수행합니다.



ODX 복사 작업을 오프로드하는 데 장애가 발생하면 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기 및 쓰기로 다시 이동됩니다. 마찬가지로, 대상 CIFS 서버가 ODX 또는 ODX를 지원하지 않을 경우 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기 및 쓰기로 다시 돌아갑니다.

## ODX 사용을 위한 요구사항

복사 오프로드를 SVM(스토리지 가상 머신)과 함께 사용하려면 먼저 특정 요구사항을 알고 있어야 합니다.

### ONTAP 버전 요구 사항

ONTAP는 복사 오프로드를 위한 ODX를 지원합니다.

### SMB 버전 요구 사항

- ONTAP는 SMB 3.0 이상을 지원하는 ODX를 지원합니다.
- ODX를 사용하려면 CIFS 서버에서 SMB 3.0을 설정해야 함:
  - ODX를 사용하도록 설정하면 SMB 3.0도 사용할 수 없습니다.
  - SMB 3.0을 비활성화하면 ODX도 비활성화됩니다.

### Windows 서버 및 클라이언트 요구 사항

복사 오프로드를 위해 ODX를 사용하려면 Windows 클라이언트에서 이 기능을 지원해야 합니다.

를 클릭합니다 ["NetApp 상호 운용성 매트릭스"](#)지원되는 Windows 클라이언트에 대한 최신 정보를 제공합니다.

### 볼륨 요구 사항

- 소스 볼륨은 최소 1.25GB여야 합니다.
  - 압축 볼륨을 사용하는 경우 압축 유형은 적응 가능해야 하며 압축 그룹 크기 8K만 지원됩니다.
- 보조 압축 유형은 지원되지 않습니다.

## ODX 사용 지침

복사 오프로드에 ODX를 사용하려면 먼저 지침을 숙지하고 있어야 합니다. 예를 들어, ODX를 사용할 수 있는 볼륨 유형을 파악하고 클러스터 내부 및 클러스터 간 ODX 고려 사항을 파악해야 합니다.

### 볼륨 지침

- 다음과 같은 볼륨 구성에서는 복사 오프로드에 ODX를 사용할 수 없습니다.
    - 소스 볼륨 크기가 1.25GB 미만입니다
- ODX를 사용하려면 볼륨 크기가 1.25GB 이상이어야 합니다.
- 읽기 전용 볼륨입니다

ODX는 로드 공유 미러 또는 SnapMirror 또는 SnapVault 대상 볼륨에 상주하는 파일 및 폴더에 사용되지 않습니다.

- 소스 볼륨 중복 제거가 수행되지 않은 경우
- ODX 복사본은 클러스터 내 복사본에만 지원됩니다.

ODX를 사용하여 파일 또는 폴더를 다른 클러스터의 볼륨으로 복사할 수는 없습니다.

#### 기타 지침

- SMB 환경에서 복사 오프로드에 ODX를 사용하려면 파일이 256KB 이상이어야 합니다.

작은 파일은 기존 복사 작업을 사용하여 전송됩니다.

- ODX 복사 오프로드는 복제 프로세스의 일부로 중복 제거를 사용합니다.

데이터를 복사하거나 이동할 때 SVM 볼륨에서 중복 제거를 수행하지 않으려면 해당 SVM에서 ODX 복사 오프로드를 해제해야 합니다.

- ODX를 지원하려면 데이터 전송을 수행하는 애플리케이션에 데이터를 기록해야 합니다.

ODX를 지원하는 애플리케이션 작업은 다음과 같습니다.

- VHD(가상 하드 디스크) 생성 및 변환, Snapshot 복사본 관리, 가상 시스템 간 파일 복사와 같은 Hyper-V 관리 작업입니다
- Windows 탐색기 작업
- Windows PowerShell 복사 명령
- Windows 명령 프롬프트 복사 명령

Windows 명령 프롬프트의 Robocopy는 ODX를 지원합니다.



ODX를 지원하는 Windows 서버 또는 클라이언트에서 애플리케이션이 실행되고 있어야 합니다.

+ Windows 서버 및 클라이언트에서 지원되는 ODX 애플리케이션에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

#### 관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

#### ODX의 사용 사례

ODX가 성능 이점을 제공하는 상황을 파악할 수 있도록 SVM에서 ODX를 사용하는 사용 사례를 알고 있어야 합니다.

ODX를 지원하는 Windows 서버 및 클라이언트는 원격 서버 간에 데이터를 복사하는 기본 방법으로 복사 오프로드를 사용합니다. Windows 서버 또는 클라이언트가 ODX를 지원하지 않거나 ODX 복사 오프로드가 어느 시점에서든 장애가 발생하면 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기/쓰기로 다시 돌아갑니다.

ODX 복사 및 이동 사용을 지원하는 사용 사례는 다음과 같습니다.

- 체내

소스 및 대상 파일 또는 LUN이 동일한 볼륨 내에 있습니다.

- 볼륨 간, 동일한 노드, 동일한 SVM

소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- 볼륨 간, 다른 노드, 동일한 SVM

소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- SVM 간, 동일한 노드

소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- SVM 간, 다른 노드

소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- 클러스터 간

소스 및 타겟 LUN은 클러스터 전반의 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 이 기능은 SAN에만 지원되며 CIFS에는 사용할 수 없습니다.

다음과 같은 몇 가지 특별한 사용 사례가 있습니다.

- ONTAP ODX를 구현하면 ODX를 사용하여 SMB 공유와 FC 또는 iSCSI 연결 가상 드라이브 간에 파일을 복사할 수 있습니다.

SMB 공유와 LUN이 동일한 클러스터에 존재하는 경우, ODX를 지원하는 Windows 탐색기, Windows CLI 또는 PowerShell, Hyper-V 또는 기타 애플리케이션을 사용하여 SMB 공유와 연결된 LUN 간에 ODX 복사 오프로드를 사용하여 파일을 원활하게 복사 또는 이동할 수 있습니다.

- Hyper-V는 ODX 복사 오프로드를 위한 몇 가지 추가 사용 사례를 제공합니다.

- Hyper-V에서 ODX 복사 오프로드 패스스루를 사용하여 VHD(가상 하드 디스크) 파일 내부 또는 VHD 파일 간에 데이터를 복사하거나, 매핑된 SMB 공유와 동일한 클러스터 내에서 연결된 iSCSI LUN 간에 데이터를 복사할 수 있습니다.

이렇게 하면 게스트 운영 체제에서 복제본을 기본 스토리지로 전달할 수 있습니다.

- 고정 크기의 VHD를 생성할 때 ODX는 잘 알려진 제로화 토큰을 사용하여 0으로 디스크를 초기화하는 데 사용됩니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드가 가상 머신 스토리지 마이그레이션에 사용됩니다.





Hyper-V를 사용한 ODX 복사 오프로드 패스쓰루 사용 사례를 활용하려면 게스트 운영 체제가 ODX를 지원하고, 게스트 운영 체제 디스크는 ODX를 지원하는 스토리지(SMB 또는 SAN)를 통해 지원되는 SCSI 디스크여야 합니다. 게스트 운영 체제의 IDE 디스크는 ODX 패스쓰루를 지원하지 않습니다.

## ODX를 설정 또는 해제합니다

스토리지 가상 시스템(SVM)에서 ODX를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본적으로 SMB 3.0도 사용하도록 설정된 경우 ODX 복사 오프로드를 지원합니다.

시작하기 전에

SMB 3.0을 활성화해야 합니다.

이 작업에 대해

SMB 3.0을 비활성화하면 ONTAP도 SMB ODX를 비활성화합니다. SMB 3.0을 다시 설정하는 경우 SMB ODX를 수동으로 다시 설정해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

ODX 복사 오프로드 기능을 사용하려면...	명령 입력...
활성화됨	'vserver cifs options modify -vserver vserver_name -copy -offload -enabled true'
사용 안 함	'vserver cifs options modify -vserver vserver_name -copy -offload -enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 SVM VS1 에서 ODX 복사 오프로드를 활성화합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

관련 정보

자동 위치로 **SMB** 자동 노드 조회를 제공하여 클라이언트 응답 시간을 단축합니다

자동 위치 개요를 통해 **SMB** 자동 노드 조회를 제공하여 클라이언트 응답 시간을 단축합니다

자동 위치에서는 SMB 자동 노드 조회를 사용하여 스토리지 가상 시스템(SVM)에서 SMB 클라이언트 성능을 높입니다. 자동 노드 조수는 요청 클라이언트를 데이터가 상주하는 볼륨을 호스팅하는 노드 SVM의 LIF로 자동으로 리디렉션하여 클라이언트 응답 시간을 향상할 수 있습니다.

SMB 클라이언트가 SVM에서 호스팅된 SMB 공유에 연결할 경우, 요청된 데이터를 소유하지 않은 노드에 있는 LIF를 사용하여 연결할 수 있습니다. 클라이언트가 연결된 노드는 클러스터 네트워크를 사용하여 다른 노드가 소유한 데이터에 액세스합니다. SMB 연결이 요청된 데이터를 포함하고 있는 노드에 있는 LIF를 사용하면 클라이언트에서 더 빠른 응답 시간을 경험할 수 있습니다.

- ONTAP은 Microsoft DFS 조회를 사용하여 SMB 클라이언트에 네임스페이스에서 요청된 파일 또는 폴더가 다른 곳에 호스팅된다는 사실을 알리는 이 기능을 제공합니다.

노드가 데이터를 포함하는 노드에 SVM LIF가 있다고 판단하면 노드를 전문의에게 의뢰합니다.

- IPv4 및 IPv6 LIF IP 주소에 대해 자동 노드 조회가 지원됩니다.
- 조인은 클라이언트가 연결되는 공유 루트의 위치를 기반으로 합니다.
- SMB 협상 중에 불합격입니다.

연결이 설정되기 전에 의뢰합니다. ONTAP가 SMB 클라이언트를 타겟 노드로 참조하면 연결이 연결되고 클라이언트는 해당 시점부터 참조된 LIF 경로를 통해 데이터에 액세스합니다. 이렇게 하면 클라이언트가 데이터에 더 빠르게 액세스할 수 있고 추가 클러스터 통신을 피할 수 있습니다.



공유가 여러 연결 지점을 거치는 경우 일부 접합부가 다른 노드에 포함된 볼륨에 연결되는 경우 공유 내의 데이터가 여러 노드로 분산됩니다. ONTAP는 공유의 루트에 대해 로컬인 조회를 제공하므로 ONTAP는 이러한 비 로컬 볼륨에 포함된 데이터를 검색하기 위해 클러스터 네트워크를 사용해야 합니다. 이러한 유형의 네임스페이스 아키텍처를 사용하면 자동 노드 조회가 성능에 큰 이점을 제공하지 않을 수 있습니다.

데이터를 호스팅하는 노드에 사용 가능한 LIF가 없는 경우 ONTAP은 클라이언트가 선택한 LIF를 사용하여 연결을 설정합니다. SMB 클라이언트가 파일을 연 후에는 동일한 참조 연결을 통해 계속 파일에 액세스합니다.

어떤 이유로든 CIFS 서버가 조회를 수행할 수 없는 경우 SMB 서비스가 중단되지 않습니다. SMB 연결은 자동 노드 조회가 활성화되지 않은 것처럼 설정됩니다.

관련 정보

[Microsoft 원격 복제 성능 향상](#)

자동 노드 조회를 사용하기 위한 요구 사항 및 지침

SMB 자동 노드 조회를 사용하려면 `_autolocation_` 이라고도 하며, 이 기능을 지원하는 ONTAP 버전을 비롯한 특정 요구 사항을 알고 있어야 합니다. 또한 지원되는 SMB 프로토콜 버전 및 기타 특정 특별 지침에 대해서도 알아야 합니다.

## ONTAP 버전 및 라이선스 요구 사항

- 클러스터의 모든 노드는 자동 노드 조회를 지원하는 ONTAP 버전을 실행하고 있어야 합니다.
- 자동 위치 정보를 사용하려면 SMB 공유에서 Widelink를 활성화해야 합니다.
- CIFS에 대한 라이선스가 있어야 하며 SMB 서버가 SVM에 있어야 합니다. SMB 라이선스는 에 포함되어 있습니다 ["ONTAP 1 을 참조하십시오"](#). ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

## SMB 프로토콜 버전 요구 사항

- SVM의 경우 ONTAP는 모든 SMB 버전에서 자동 노드 조회를 지원합니다.

## SMB 클라이언트 요구 사항

ONTAP에서 지원하는 모든 Microsoft 클라이언트는 SMB 자동 노드 조회를 지원합니다.

상호 운용성 매트릭스에는 ONTAP에서 지원하는 Windows 클라이언트에 대한 최신 정보가 포함되어 있습니다.

["NetApp 상호 운용성 매트릭스 툴"](#)

## 데이터 LIF 요구사항

데이터 LIF를 SMB 클라이언트를 위한 잠재 고객으로 사용하려면 NFS와 CIFS를 모두 사용하도록 설정된 데이터 LIF를 생성해야 합니다.

타겟 노드에 NFS 프로토콜에만 사용하도록 설정된 데이터 LIF가 있거나 SMB 프로토콜에 대해서만 사용하도록 설정된 데이터 LIF가 있는 경우 자동 노드 조회가 작동하지 않을 수 있습니다.

이 요구 사항이 충족되지 않으면 데이터 액세스가 영향을 받지 않습니다. SMB 클라이언트는 클라이언트가 SVM에 연결할 때 사용한 원래 LIF를 사용하여 공유를 매핑합니다.

## 참조된 SMB 연결을 만들 때 NTLM 인증 요구 사항

NTLM 인증은 CIFS 서버가 포함된 도메인 및 자동 노드 조회를 사용하려는 클라이언트가 포함된 도메인에서 허용되어야 합니다.

SMB 서버는 조회를 수행할 때 Windows 클라이언트에 대한 IP 주소를 참조합니다. NTLM 인증은 IP 주소를 사용하여 연결할 때 사용되므로 Kerberos 인증은 참조된 연결에 대해 수행되지 않습니다.

이는 Kerberos(service/netbios name, service/FQDN) 형태의 서비스 주체 이름을 Windows 클라이언트가 생성할 수 없기 때문에 클라이언트가 Kerberos 티켓을 서비스에 요청할 수 없다는 뜻입니다.

## 홈 디렉토리 기능과 함께 자동 노드 조회를 사용하는 지침

공유가 홈 디렉토리 공유 속성을 사용하여 구성된 경우 홈 디렉토리 구성에 대해 하나 이상의 홈 디렉토리 검색 경로가 구성될 수 있습니다. 검색 경로는 SVM 볼륨을 포함하는 각 노드에 포함된 볼륨을 가리킬 수 있습니다. 클라이언트는 추천을 받으며 액티브 로컬 데이터 LIF가 사용 가능한 경우 홈 사용자의 홈 디렉토리에 로컬로 연결된 참조된 LIF를 통해 연결됩니다.

SMB 1.0 클라이언트가 자동 노드 조회가 설정된 동적 홈 디렉토리에 액세스하는 경우 지침이 있습니다. 이는 SMB 1.0 클라이언트가 인증을 받기 전에 자동 노드 조회를 필요로 하기 때문입니다. 이는 SMB 서버가 사용자 이름을 가지기 전입니다. 그러나 SMB 1.0 클라이언트에서 SMB 홈 디렉토리 액세스가 올바르게 작동하는 경우는 다음과 같습니다.

- SMB 홈 디렉토리는 ""w"(Windows 사용자 이름) 또는 ""u"(매핑된 UNIX 사용자 이름)와 같은 단순 이름을 사용하도록 구성되어 있으며 ""d\w"(domain-name\user-name)와 같은 도메인 이름 스타일 이름은 사용하지 않습니다.
- 홈 디렉토리 공유를 생성할 때 CIFS 홈 디렉토리 공유 이름은 ""home""과 같은 정적 이름이 아니라 변수("""w" 또는 ""u")로 구성됩니다.

SMB 2.x 및 SMB 3.0 클라이언트의 경우 자동 노드 조회를 사용하여 홈 디렉토리에 액세스할 때 특별한 지침이 없습니다.

기존에 연결된 연결이 있는 **CIFS** 서버에서 자동 노드 조회를 해제하는 지침입니다

이 옵션이 설정된 후 자동 노드 조회를 사용하지 않도록 설정하면 현재 참조된 LIF에 연결된 클라이언트가 계속 연결된 상태로 유지됩니다. ONTAP은 DFS 조회를 SMB 자동 노드 조정의 메커니즘으로 사용하므로, 클라이언트의 캐시된 DFS 참조 시간이 초과될 때까지 이 옵션을 비활성화한 후에 클라이언트가 참조된 LIF에 다시 연결할 수도 있습니다. 자동 노드 조회를 지원하지 않는 ONTAP 버전으로 되돌리는 경우에도 마찬가지입니다. 클라이언트는 클라이언트의 캐시에서 DFS 참조 시간이 초과될 때까지 계속 조회를 사용합니다.

Autolocation은 SMB 자동 노드 조회를 사용하여 SVM의 데이터 볼륨을 소유하는 노드의 LIF에 클라이언트를 위탁하여 SMB 클라이언트의 성능을 높입니다. SMB 클라이언트가 SVM에서 호스팅되는 SMB 공유에 연결할 경우, 요청된 데이터를 소유하지 않고 클러스터 인터커넥트 네트워크를 사용하여 데이터를 검색하는 노드에서 LIF를 사용하여 연결할 수 있습니다. SMB 연결이 요청된 데이터를 포함하고 있는 노드에 있는 LIF를 사용하는 경우 클라이언트는 더 빠른 응답 시간을 경험할 수 있습니다.

ONTAP은 Microsoft DFS(분산 파일 시스템) 조회를 사용하여 SMB 클라이언트에 네임스페이스에서 요청된 파일 또는 폴더가 다른 곳에 호스팅된다는 사실을 알려 주는 이 기능을 제공합니다. 노드가 데이터를 포함하는 노드에 SVM LIF가 있다고 판단하면 노드를 전문의에게 의뢰합니다. 조인은 클라이언트가 연결되는 공유 루트의 위치를 기반으로 합니다.

SMB 협상 중에 불합격입니다. 연결이 설정되기 전에 의뢰합니다. ONTAP가 SMB 클라이언트를 타겟 노드로 참조하면 연결이 연결되고 클라이언트는 해당 시점부터 참조된 LIF 경로를 통해 데이터에 액세스합니다. 이렇게 하면 클라이언트가 데이터에 더 빠르게 액세스할 수 있고 추가 클러스터 통신을 피할 수 있습니다.

**Mac OS** 클라이언트에서 자동 노드 조회를 사용하는 방법에 대한 지침입니다

Mac OS X 클라이언트는 Microsoft의 DFS(Distributed File System)를 지원하지만 SMB 자동 노드 조회를 지원하지 않습니다. Windows 클라이언트는 SMB 공유에 연결하기 전에 DFS 참조 요청을 합니다. ONTAP은 요청된 데이터를 호스팅하는 동일한 노드에 있는 데이터 LIF를 지칭하여 클라이언트 응답 시간을 개선합니다. Mac OS는 DFS를 지원하지만 Mac OS 클라이언트는 이 영역의 Windows 클라이언트와 정확히 작동하지 않습니다.

관련 정보

[ONTAP에서 동적 홈 디렉토리를 활성화하는 방법](#)

["네트워크 관리"](#)

["NetApp 상호 운용성 매트릭스 툴"](#)

**SMB** 자동 노드 조회를 지원합니다

SMB 자동 노드 조회를 활성화하기 전에 특정 ONTAP 기능이 조회를 지원하지 않는다는 점을 알아야 합니다.

- 다음 유형의 볼륨은 SMB 자동 노드 조회를 지원하지 않습니다.

- 로드 공유 미러의 읽기 전용 구성원입니다
- 데이터 보호 미러의 타겟 볼륨입니다
- 노드 조회가 LIF 이동 옆에서 이동하지 않습니다.

클라이언트가 SMB 2.x 또는 SMB 3.0 연결을 통해 위탁된 연결을 사용 중이고 데이터 LIF가 중단 없이 이동되는 경우, LIF가 더 이상 데이터에 로컬이 아니어도 클라이언트는 계속 동일한 연결 연결을 사용합니다.

- 노드 조회가 볼륨 이동 옆에서 이동하지 않습니다.

클라이언트가 SMB 연결을 통해 참조된 연결을 사용하고 있고 볼륨 이동이 발생하는 경우, 클라이언트는 볼륨이 데이터 LIF와 같은 노드에 더 이상 존재하지 않더라도 계속해서 동일한 연결 연결을 사용합니다.

## SMB 자동 노드 조회를 설정하거나 해제합니다

SMB 자동 노드 조회를 활성화하여 SMB 클라이언트 액세스 성능을 높일 수 있습니다. ONTAP가 SMB 클라이언트에 조회를 하지 않도록 하려면 자동 노드 조회를 사용하지 않도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버는 SVM(스토리지 가상 머신)에서 구성 및 실행해야 합니다.

이 작업에 대해

SMB 자동 노드 조회 기능은 기본적으로 비활성화되어 있습니다. 필요에 따라 각 SVM에서 이 기능을 활성화 또는 비활성화할 수 있습니다.

이 옵션은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 필요에 따라 SMB 자동 노드 조회를 설정하거나 해제합니다.

SMB 자동 노드 조회를 원하는 경우...	다음 명령을 입력합니다...
활성화됨	'vserver cifs options modify -vserver vserver_name -is-referral-enabled true'
사용 안 함	'vserver cifs options modify -vserver vserver_name -is-referral-enabled false'

옵션 설정은 새 SMB 세션에 적용됩니다. 기존 연결이 있는 클라이언트는 기존 캐시 시간 초과가 만료될 때만 노드 조회를 활용할 수 있습니다.

3. 'Set-Privilege admin'으로 설정

관련 정보

[사용 가능한 SMB 서버 옵션](#)

통계를 사용하여 자동 노드 조회 활동을 모니터링합니다

SMB 연결 조회 수를 확인하려면 '통계' 명령어를 사용해 자동 노드 조회 활동을 모니터링할 수 있다. 조회를 모니터링하면 공유를 호스팅하는 노드에서 자동 조회가 접속을 찾는 범위와 CIFS 서버의 공유에 대한 로컬 액세스를 더 잘 제공할 수 있도록 데이터 LIF를 재분산해야 하는지 여부를 확인할 수 있습니다.

이 작업에 대해

"CIFS" 객체는 SMB 자동 노드 조회를 모니터링할 때 유용한 고급 권한 수준의 여러 카운터를 제공합니다.

- 'node\_referral\_발급'

공유 루트의 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 클라이언트가 연결된 후 공유 루트 노드에 대한 조회를 실행한 클라이언트 수입입니다.

- 'node\_referral\_local'

공유 루트를 호스팅하는 동일한 노드에서 호스팅되는 LIF를 사용하여 연결된 클라이언트의 수입입니다. 로컬 액세스는 일반적으로 최적의 성능을 제공합니다.

- 'node\_referral\_not\_possible'

공유 루트의 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 연결한 후 공유 루트를 호스팅하는 노드에 아직 위탁하지 않은 클라이언트 수입입니다. 이는 공유 루트의 노드에 대한 활성 데이터 LIF를 찾을 수 없기 때문입니다.

- 'node\_referral\_remote'

공유 루트를 호스팅하는 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 연결된 클라이언트 수입입니다. 원격 액세스로 인해 성능이 저하될 수 있습니다.

특정 기간(샘플)에 대한 데이터를 수집 및 확인하여 스토리지 가상 시스템(SVM)에 대한 자동 노드 참조 통계를 모니터링할 수 있습니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 성능 추세를 파악할 수 있습니다.



'통계' 명령을 통해 수집한 정보를 평가하고 사용하려면 사용자 환경에서 클라이언트의 분포를 이해해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. '통계' 명령어를 이용하여 자동 노드 조회 통계를 볼 수 있다.

이 예제에서는 샘플링된 기간에 대한 데이터를 수집하고 확인하여 자동 노드 참조 통계를 보여 줍니다.

- a. 'stantics start-object cifs-instance vs1-sample-id sample1' 컬렉션을 시작합니다

```
Statistics collection is being started for Sample-id: sample1
```

- b. 원하는 수집 시간이 경과할 때까지 기다립니다.

c. '스타티틱스 스톱-시료-ID sample1' 컬렉션을 중단한다

```
Statistics collection is being stopped for Sample-id: sample1
```

d. 자동 노드 참조 통계: 'stattics show -sample-id sample1-counter \* node \*'를 봅니다

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

Counter	Value
node_name	node1
node_referral_issued	0
node_referral_local	1
node_referral_not_possible	2
node_referral_remote	2
...	
node_name	node2
node_referral_issued	2
node_referral_local	1
node_referral_not_possible	0
node_referral_remote	2
...	

SVM VS1에 참여하는 모든 노드의 카운터를 출력합니다. 이 예에서는 자동 노드 조회 통계와 관련된 출력 필드만 제공합니다.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

[통계를 표시합니다](#)

["성능 모니터링 설정"](#)

**Windows** 클라이언트를 사용하여 클라이언트 측 **SMB** 자동 노드 조회 정보를 모니터링합니다

클라이언트의 관점에서 어떤 조회를 수행할지 결정하려면 Windows dutil.exe를 사용할 수 있습니다.

Windows 7 이상의 클라이언트에서 사용할 수 있는 RSAT(원격 서버 관리 도구) 키트에는 Dsutil.exe가 포함되어 있습니다. 이 유틸리티를 사용하면 추천 캐시의 내용에 대한 정보를 표시하고 클라이언트가 현재 사용하고 있는 각 추천 정보에 대한 정보를 볼 수 있습니다. 이 유틸리티를 사용하여 클라이언트의 조회 캐시를 지울 수도 있습니다. 자세한

내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

## 액세스 기반 열거를 사용하여 공유에 대한 폴더 보안을 제공합니다

액세스 기반 열거 개요를 사용하여 공유에 대한 폴더 보안을 제공합니다

SMB 공유에서 ABE(Access-Based Enumeration)를 사용하면 공유 내에 포함된 폴더나 파일에 액세스할 수 있는 권한이 없는 사용자(개인 또는 그룹 권한 제한 사용 여부)는 공유 자체가 표시되더라도 공유 리소스가 해당 환경에 표시되지 않습니다.

일반 공유 속성을 사용하면 공유에 포함된 파일 또는 폴더를 보거나 수정할 수 있는 권한이 있는 사용자(개별 또는 그룹)를 지정할 수 있습니다. 그러나 공유 내의 폴더나 파일이 액세스 권한이 없는 사용자에게 표시되는지 여부를 제어할 수는 없습니다. 이러한 폴더 또는 공유 내의 파일 이름이 개발 중인 고객 또는 제품 이름과 같은 중요한 정보를 설명하는 경우 문제가 발생할 수 있습니다.

ABE(Access-Based Enumeration)는 공유 속성을 확장하여 공유 내의 파일 및 폴더 열거를 포함합니다. 따라서 ABE를 사용하면 사용자 액세스 권한에 따라 공유 내의 파일 및 폴더 표시를 필터링할 수 있습니다. 즉, 공유 자체는 모든 사용자에게 표시되지만 공유 내의 파일과 폴더는 지정된 사용자에게 표시되거나 숨겨집니다. 업무 공간의 중요한 정보를 보호하는 것 외에도, ABE를 사용하면 전체 콘텐츠 범위에 액세스할 필요가 없는 사용자에게 혜택을 제공하기 위해 대규모 디렉터리 구조의 표시를 단순화할 수 있습니다. 예를 들어 공유 자체는 모든 사용자에게 표시되지만 공유 내의 파일과 폴더는 표시하거나 숨길 수 있습니다.

에 대해 자세히 알아보십시오 "SMB/CIFS 액세스 기반 열거 사용 시 성능에 미치는 영향".

**SMB** 공유에서 액세스 기반 열거를 설정하거나 해제합니다

SMB 공유에서 ABE(Access-Based Enumeration)를 설정하거나 해제하여 사용자가 액세스 권한이 없는 공유 리소스를 볼 수 없도록 하거나 허용할 수 있습니다.

이 작업에 대해

기본적으로 ABE는 비활성화되어 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
새 공유에서 ABE를 활성화합니다	'vserver cifs share create -vserver vservice_name -share-name -path path path -share-properties access-based-enumeration' SMB 공유를 생성할 때 추가 선택적 공유 설정 및 추가 공유 속성을 지정할 수 있습니다. 자세한 내용은 'vserver cifs share create' 명령에 대한 man 페이지를 참조하십시오.



원하는 작업	명령 입력...
기존 공유에서 ABE를 활성화합니다	'vserver cifs 공유 속성 add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration' 기존 공유 속성은 보존됩니다. ABE 공유 속성은 기존 공유 속성 목록에 추가됩니다.
기존 공유에서 ABE를 비활성화합니다	'vserver cifs share properties remove - vserver vserver_name -share-name share_name -share -properties access-based-enumeration' 다른 공유 속성은 보존됩니다. 공유 속성 목록에서 ABE 공유 속성만 제거됩니다.

2. 'vserver cifs share show' 명령을 사용하여 공유 구성이 올바른지 확인합니다.

예

다음 예에서는 SVM VS1 에서 /sales 경로를 사용하여 "sale"이라는 이름의 ABE SMB 공유를 생성합니다. 공유는 공유 속성으로 '액세스 기반 열거'로 만들어집니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

Vserver: vs1
Share: sales
CIFS Server NetBIOS Name: VS1
Path: /sales
Share Properties: access-based-enumeration
                  oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

다음 예제에서는 "data2"라는 SMB 공유에 "액세스 기반 열거" 공유 속성을 추가합니다.

```
cluster1::> vservers cifs share properties add -vservers vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vservers cifs share show -vservers vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changeNotify,access-based-enumeration
```

## 관련 정보

### 기존 SMB 공유에서 공유 속성 추가 또는 제거

**Windows** 클라이언트에서 액세스 기반 열거를 사용하거나 사용하지 않도록 설정합니다

Windows 클라이언트에서 SMB 공유에 대해 ABE(액세스 기반 열거)를 설정하거나 해제할 수 있습니다. 그러면 CIFS 서버에 연결하지 않고도 이 공유 설정을 구성할 수 있습니다.



새 버전의 Windows Server 및 Windows 클라이언트에서는 abecmd 유틸리티를 사용할 수 없습니다. 이 제품은 Windows Server 2008의 일부로 출시되었습니다. 2020년 1월 14일에 Windows Server 2008에 대한 지원이 종료되었습니다.

## 단계

1. ABE를 지원하는 Windows 클라이언트에서 'abecmd[/enable|/disable][server cifs\_server\_name][all|share\_name]' 명령을 입력합니다

"abecmd" 명령에 대한 자세한 내용은 Windows 클라이언트 설명서를 참조하십시오.

# NFS 및 SMB 파일 및 디렉토리 명명 종속성

## NFS 및 SMB 파일 및 디렉토리 이름 지정 종속성 개요

파일 및 디렉토리 명명 규칙은 ONTAP 클러스터 및 클라이언트의 언어 설정과 함께 네트워크 클라이언트의 운영 체제 및 파일 공유 프로토콜에 따라 다릅니다.

운영 체제 및 파일 공유 프로토콜에는 다음이 결정됩니다.

- 문자 파일 이름에 사용할 수 있습니다
- 파일 이름의 대/소문자 구분

ONTAP는 ONTAP 릴리즈별 파일, 디렉토리 및 qtree 이름에서 멀티바이트 문자를 지원합니다.

문자 파일 또는 디렉토리 이름에 사용할 수 있습니다

다른 운영 체제를 사용하는 클라이언트에서 파일 또는 디렉토리에 액세스하는 경우 두 운영 체제 모두에서 유효한 문자를 사용해야 합니다.

예를 들어 UNIX를 사용하여 파일 또는 디렉토리를 생성하는 경우 MS-DOS 파일 또는 디렉토리 이름에 콜론이 허용되지 않으므로 이름에 콜론(:)을 사용하지 마십시오. 유효한 문자의 제한 사항은 운영 체제마다 다르므로 금지된 문자에 대한 자세한 내용은 클라이언트 운영 체제 설명서를 참조하십시오.

## 다중 프로토콜 환경에서 파일 및 디렉토리 이름의 대/소문자를 구분하십시오

파일 및 디렉토리 이름은 NFS 클라이언트의 경우 대/소문자를 구분하며, SMB 클라이언트의 경우 대/소문자를 구분하지 않지만 대/소문자를 구분합니다. SMB 공유를 생성하는 동안 그리고 공유 내의 데이터에 액세스할 때 경로를 지정할 때 취해야 할 조치와 멀티 프로토콜 환경에 미치는 영향을 이해해야 합니다.

SMB 클라이언트가 testdir라는 디렉토리를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 testdir로 표시합니다. 그러나 SMB 사용자가 나중에 디렉터리 이름 testdir을 만들려고 하면 해당 이름이 SMB 클라이언트에 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 "testdir"이라는 디렉토리를 생성할 경우 NFS 및 SMB 클라이언트는 다음과 같이 디렉토리 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 디렉토리 이름이 대/소문자를 구분하기 때문에 디렉토리 이름이 생성될 때 testdir와 testDIR 같은 두 디렉토리 이름을 모두 볼 수 있습니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 디렉토리를 구분합니다. 한 디렉토리에 기본 파일 이름이 있습니다. 추가 디렉토리에는 8.3 파일 이름이 할당됩니다.
  - SMB 클라이언트에서는 testdir과 testDIR~1이 표시됩니다.
  - ONTAP는 두 디렉토리를 구분하기 위해 'TESTDIR~1' 디렉토리 이름을 생성한다.

이 경우 SVM(스토리지 가상 머신)에서 공유를 생성하거나 수정하는 동안 공유 경로를 지정할 때 8.3 이름을 사용해야 합니다.

마찬가지로 SMB 클라이언트가 test.txt를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 test.txt로 표시합니다. 그러나 SMB 사용자가 나중에 Test.txt를 생성하려고 하면 SMB 클라이언트에 해당 이름이 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 Test.txt라는 파일을 만들면 NFS 및 SMB 클라이언트는 다음과 같이 파일 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 파일 이름이 대/소문자를 구분하기 때문에 이름이 test.txt와 Test.txt로 만들어지면 두 파일 이름이 모두 표시됩니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 파일을 구분합니다. 한 파일에 기본 파일 이름이 있습니다. 8.3 파일 이름이 추가로 할당됩니다.
  - SMB 클라이언트의 경우 test.txt와 test~1.TXT가 표시됩니다.
  - ONTAP는 두 파일을 구별하기 위해 'test~1.TXT' 파일 이름을 만듭니다.



SVM CIFS 문자 매핑 명령을 사용하여 문자 매핑을 설정하거나 수정한 경우 일반적으로 대/소문자를 구분하지 않는 Windows 조화가 대/소문자를 구분합니다.

## ONTAP에서 파일 및 디렉터리 이름을 만드는 방법

ONTAP는 SMB 클라이언트에서 액세스할 수 있는 디렉터리인 원래 긴 이름과 8.3 형식의 이름을 사용하여 파일 또는 디렉터리의 이름을 두 개 생성하고 유지합니다.

파일 또는 디렉토리 이름이 8자 이름 또는 3자 확장자 제한(파일의 경우)을 초과하는 경우, ONTAP는 다음과 같이 8.3

형식 이름을 생성합니다.

- 이름이 6자를 초과하면 원본 파일 또는 디렉터리 이름이 6자로 잘립니다.
- 잘려서 더 이상 고유하지 않은 파일 또는 디렉터리 이름에 물결표(~)와 숫자(1 - 5)를 추가합니다.

비슷한 이름이 5개 이상 있어 숫자가 부족하면 원래 이름과 아무런 관계가 없는 고유한 이름이 만들어집니다.

- 파일의 경우 파일 확장명이 3자로 잘립니다.

예를 들어, NFS 클라이언트가 'specifications.html'이라는 파일을 생성할 경우 ONTAP에서 생성한 8.3 형식 파일 이름은 'specif~1.htm'입니다. 이 이름이 이미 있는 경우 ONTAP에서는 파일 이름 끝에 다른 번호를 사용합니다. 예를 들어, NFS 클라이언트가 'specifications\_new.html'이라는 다른 파일을 만들 경우 'specifications\_new.html'의 8.3 형식은 'specif~2.htm'입니다.

## ONTAP에서 멀티바이트 파일, 디렉터리 및 **qtree** 이름을 처리하는 방식

ONTAP 9.5부터 4바이트 UTF-8 인코딩 이름을 지원하므로 BMP(기본 다국어 플레인) 외부의 유니코드 보조 문자를 포함하는 파일, 디렉터리 및 트리 이름을 만들고 표시할 수 있습니다. 이전 릴리스에서는 이러한 보조 문자가 멀티 프로토콜 환경에서 올바르게 표시되지 않았습니다.

4바이트 UTF-8 인코딩된 이름을 지원하기 위해 새 `_utf8mb4_language` 코드를 "vserver" 및 "volume" 명령 제품군에 사용할 수 있습니다.

다음 방법 중 하나로 새 볼륨을 만들어야 합니다.

- 볼륨 '-language' 옵션을 명시적으로 설정하는 것은 'volume create-language utf8mb4{...}'입니다
- 옵션을 위해 생성되거나 수정된 SVM에서 볼륨 '-language' 옵션을 상속합니다: 'vserver[create|modify] -language utf8mb4{...}"volume create{...}'
- ONTAP 9.6 이하 버전에서는 utf8mb4 지원을 위한 기존 볼륨을 수정할 수 없습니다. 새로운 utf8mb4 지원 볼륨을 생성한 다음 클라이언트 기반 복사 툴을 사용하여 데이터를 마이그레이션해야 합니다.

utf8mb4 지원을 위해 SVM을 업데이트할 수 있지만 기존 볼륨에 원래 언어 코드가 유지됩니다.

ONTAP 9.7P1 이상을 사용 중인 경우 지원 요청을 통해 utf8mb4에 대한 기존 볼륨을 수정할 수 있습니다. 자세한 내용은 [참조하십시오 "ONTAP에서 생성한 후 볼륨 언어를 변경할 수 있습니까?"](#).

- ONTAP 9.8부터 를 사용할 수 있습니다 [-language <Language code>] 볼륨 언어를 \*.utf-8에서 utf8mb4로 변경하는 매개 변수입니다. 볼륨의 언어를 변경하려면 [여기](#) 문의하십시오 ["NetApp 지원"](#).



4바이트 UTF-8 문자를 사용하는 LUN 이름은 현재 지원되지 않습니다.

- 유니코드 문자 데이터는 일반적으로 16비트 UTF-16(Unicode Transformation Format)을 사용하는 Windows 파일 시스템 응용 프로그램과 8비트 UTF-8(Unicode Transformation Format)을 사용하는 NFS 파일 시스템에 표시됩니다.

ONTAP 9.5 이전 버전에서는 Windows 클라이언트에서 생성한 UTF-16 보조 문자를 포함한 이름이 다른 Windows 클라이언트에 올바르게 표시되었지만 NFS 클라이언트용 UTF-8로 올바르게 변환되지 않았습니다. 마찬가지로, 생성된 NFS 클라이언트에서 UTF-8 보완 문자를 사용하는 이름은 Windows 클라이언트의 UTF-16으로 올바르게 변환되지 않았습니다.

- ONTAP 9.4 이하를 실행하는 시스템에서 유효하거나 잘못된 보조 문자가 포함된 파일 이름을 만들면 ONTAP가 파일 이름을 거부하고 잘못된 파일 이름 오류를 반환합니다.

이 문제를 방지하려면 파일 이름에 BMP 문자만 사용하고 보조 문자는 사용하지 마십시오. 또는 ONTAP 9.5 이상으로 업그레이드하십시오.

ONTAP 9부터는 qtree 이름에 유니코드 문자가 허용됩니다.

- 'volume qtree' 명령군 또는 System Manager를 사용하여 qtree 이름을 설정하거나 수정할 수 있습니다.
- Qtree 이름에는 일본어 및 중국어 문자와 같은 유니코드 형식의 멀티바이트 문자가 포함될 수 있습니다.
- ONTAP 9.5 이전 버전에서는 BMP 문자(즉, 3바이트로 표현될 수 있는 문자)만 지원되었습니다.



ONTAP 9.5 이전의 릴리즈에서는 qtree 상위 볼륨의 연결 경로에 유니코드 문자가 있는 qtree 및 디렉토리 이름이 포함될 수 있습니다. 볼륨 표시 명령은 상위 볼륨에 UTF-8 언어 설정이 있는 경우 이러한 이름을 올바르게 표시합니다. 그러나 상위 볼륨 언어가 UTF-8 언어 설정 중 하나가 아닌 경우 junction-path의 일부 부분은 숫자 NFS 대체 이름을 사용하여 표시됩니다.

- 9.5 이상 릴리즈에서는 qtree 이름이 qtree 이름으로 지원되지만 qtree가 utf8mb4에 대해 활성화된 볼륨에 있습니다.

볼륨에서 **SMB** 파일 이름 변환에 대한 문자 매핑을 구성합니다

NFS 클라이언트는 SMB 클라이언트 및 특정 Windows 애플리케이션에 유효하지 않은 문자를 포함하는 파일 이름을 생성할 수 있습니다. SMB 클라이언트가 유효하지 않은 NFS 이름의 파일에 액세스할 수 있도록 볼륨의 파일 이름 변환에 대한 문자 매핑을 구성할 수 있습니다.

이 작업에 대해

NFS 클라이언트가 생성한 파일을 SMB 클라이언트가 액세스할 때 ONTAP는 파일 이름을 찾습니다. 이름이 유효한 SMB 파일 이름이 아닌 경우(예: 포함된 콜론 ":" 문자가 있는 경우) ONTAP는 각 파일에 대해 유지되는 8.3 파일 이름을 반환합니다. 그러나 이로 인해 중요한 정보를 긴 파일 이름으로 인코딩하는 응용 프로그램에 문제가 발생합니다.

따라서 다른 운영 체제의 클라이언트 간에 파일을 공유하는 경우 두 운영 체제 모두에서 유효한 파일 이름에 문자를 사용해야 합니다.

그러나 SMB 클라이언트에 대해 유효한 파일 이름이 아닌 문자를 포함하는 파일 이름을 생성하는 NFS 클라이언트가 있는 경우, 잘못된 NFS 문자를 SMB 및 특정 Windows 애플리케이션이 허용하는 유니코드 문자로 변환하는 맵을 정의할 수 있습니다. 예를 들어, 이 기능은 CATIA MCAD 및 Mathematica 응용 프로그램과 이 요구 사항이 있는 다른 응용 프로그램을 지원합니다.

볼륨별로 문자 매핑을 구성할 수 있습니다.

볼륨에 문자 매핑을 구성할 때 다음 사항을 염두에 두어야 합니다.

- 문자 매핑이 교차점에 적용되지 않습니다.

각 접합 볼륨에 대해 문자 매핑을 명시적으로 구성해야 합니다.

- 올바르게 않거나 잘못된 문자를 나타내는 데 사용되는 유니코드 문자가 파일 이름에 일반적으로 나타나지 않는 문자인지 확인해야 합니다. 그렇지 않으면 원치 않는 매핑이 발생합니다.

예를 들어 콜론(:)을 하이픈(-)에 매핑하려고 하지만 파일 이름에 하이픈(-)이 올바르게 사용된 경우 ""a-b""라는 파일에 액세스하려는 Windows 클라이언트의 요청이 ""a:b""(원하는 결과가 아님)의 NFS 이름에 매핑됩니다.

- 문자 매핑을 적용한 후에도 매핑에 여전히 잘못된 Windows 문자가 포함되어 있으면 ONTAP는 Windows 8.3 파일 이름으로 다시 돌아갑니다.
- FPolicy 알림, NAS 감사 로그, 보안 추적 메시지에 매핑된 파일 이름이 표시됩니다.
- DP 유형의 SnapMirror 관계가 생성될 때 소스 볼륨의 문자 매핑이 대상 DP 볼륨에 복제되지 않습니다.
- 대소문자 구분: 매핑된 Windows 이름이 NFS 이름으로 전환되기 때문에 이름 조회는 NFS 의미를 따릅니다. 여기에는 NFS 조회가 대/소문자를 구분한다는 사실도 포함됩니다. 즉, 매핑된 공유에 액세스하는 응용 프로그램이 대/소문자를 구분하지 않는 Windows 동작에 의존해서는 안 됩니다. 그러나 8.3 이름은 사용할 수 있으며 대/소문자를 구분하지 않습니다.
- 부분 매핑 또는 잘못된 매핑: 이름을 매핑하여 디렉터리 열거("dir")를 수행하는 클라이언트로 반환하면 결과 유니코드 이름이 Windows 유효성을 검사합니다. 이름에 여전히 잘못된 문자가 있거나 Windows에 유효하지 않은 경우(예: "." 또는 공백으로 끝나는 경우) 잘못된 이름 대신 8.3 이름이 반환됩니다.

단계

1. 문자 매핑 구성:

```
"vserver cifs character-mapping create -vserver_vserver_name_-volume_volume_name_-mapping_mapping_text_... 를 누릅니다
```

매핑은 ""로 구분된 소스-타겟 문자 쌍 목록으로 구성됩니다. 문자는 16진수를 사용하여 입력한 유니코드 문자입니다. 예: 3C:E03C. 를 누릅니다

콜론으로 구분된 각 mapping\_text 쌍의 첫 번째 값은 번역할 NFS 문자의 16진수 값이고 두 번째 값은 SMB가 사용하는 유니코드 값입니다. 매핑 쌍은 고유해야 합니다(일대일 매핑이 있어야 함).

- 소스 매핑+

다음 표에서는 소스 매핑에 사용할 수 있는 유니코드 문자 집합을 보여 줍니다.

를 누릅니다

유니코드 문자입니다	인쇄된 문자	설명
0x01-0x19	해당 없음	인쇄할 수 없는 제어 문자입니다
0x5C		백슬래시
0x3A	:	결장
0x2A	*	별표
0x3F	?	물음표
0x22	"	인용 부호가 있습니다

유니코드 문자입니다	인쇄된 문자	설명
0x3C	를 누릅니다	보다 작음
0x3E	를 누릅니다	보다 큼
0x7C		
세로선	0xB1	±

- 타겟 매핑

U+E0000...U+F8FF 범위의 유니코드 "전용 용도 영역"에서 대상 문자를 지정할 수 있습니다.

예

다음 명령을 실행하면 SVM(스토리지 가상 시스템) VS1 에서 "data"라는 이름의 볼륨에 대한 문자 매핑이 생성됩니다.

```
cluster1::> vsriver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vsriver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

#### 관련 정보

[NAS 네임스페이스에서 데이터 볼륨 생성 및 관리](#)

### SMB 파일 이름 변환에 대한 문자 매핑을 관리하는 명령입니다

FlexVol 볼륨에서 SMB 파일 이름 변환에 사용되는 파일 문자 매핑을 생성, 수정, 정보 표시 또는 삭제하여 문자 매핑을 관리할 수 있습니다.

원하는 작업	이 명령 사용...
새 파일 문자 매핑을 만듭니다	'vsriver cifs character-mapping create'
파일 문자 매핑에 대한 정보를 표시합니다	'vsriver cifs character-mapping show'
기존 파일 문자 매핑을 수정합니다	'vsriver cifs character-mapping modify'를 참조하십시오
파일 문자 매핑을 삭제합니다	'vsriver cifs character-mapping delete'

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.

관련 정보

[볼륨에 대한 SMB 파일 이름 변환에 대한 문자 매핑 구성](#)



## 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.