SMB를 사용하여 파일 액세스를 설정합니다
ONTAP 9

NetApp
February 12, 2026

목차

SMB를 사용하여 파일 액세스를 설정합니다 1
보안 스타일을 구성합니다 1
보안 스타일이 데이터 액세스에 미치는 영향 1
ONTAP SVM 루트 볼륨에 SMB 보안 형식을 구성합니다 4
ONTAP FlexVol 볼륨에 SMB 보안 스타일을 구성합니다 4
ONTAP qtree에서 SMB 보안 스타일을 구성합니다 4
NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다 5
NAS 네임스페이스에서 ONTAP SMB 데이터 볼륨을 생성하고 관리하는 방법에 대해 알아보십시오 5
지정된 접합 지점으로 ONTAP SMB 데이터 볼륨을 생성합니다 5
접합 지점을 지정하지 않고 ONTAP SMB 데이터 볼륨을 생성합니다 6
NAS 네임스페이스에서 기존 ONTAP SMB 볼륨을 마운트하거나 마운트 해제합니다 7
ONTAP SMB 볼륨 마운트 및 접합 지점 정보를 표시합니다 9
이름 매핑을 구성합니다 10
ONTAP SMB 이름 매핑 구성에 대해 자세히 알아보십시오 10
ONTAP SMB 이름 매핑에 대해 자세히 알아보십시오 11
UNIX 사용자와 Windows 사용자 이름 간 매핑에 대한 ONTAP SMB 다중 도메인 검색에 대해 알아봅니다 11
ONTAP SMB 이름 매핑 변환 규칙에 대해 알아보십시오 13
ONTAP SMB 이름 매핑을 생성합니다 13
기본 ONTAP SMB 사용자를 구성합니다 14
SMB 이름 매핑을 관리하기 위한 ONTAP 명령 15
다중 도메인 이름 매핑 검색을 구성합니다 15
ONTAP SMB 다중 도메인 이름 매핑 검색을 사용하거나 사용하지 않도록 설정합니다 15
신뢰할 수 있는 ONTAP SMB 도메인을 재설정하고 재검색합니다 16
검색된 신뢰할 수 있는 ONTAP SMB 도메인에 대한 정보를 표시합니다 16
기본 설정 목록에서 신뢰할 수 있는 ONTAP SMB 도메인을 추가, 제거 또는 교체합니다 17
기본 설정 신뢰할 수 있는 ONTAP SMB 도메인 목록에 대한 정보를 표시합니다 19
SMB 공유를 생성하고 구성합니다 19
ONTAP SMB 공유 생성 및 구성에 대해 자세히 알아보십시오 19
기본 관리 ONTAP SMB 공유에 대해 알아봅니다 20
ONTAP SMB 공유 명명 요구사항에 대해 알아보십시오 21
멀티 프로토콜 환경에서 공유를 생성할 때의 ONTAP SMB 디렉토리 대소문자 구분 요구사항에 대해 알아보십시오 22
SMB 공유 속성을 사용합니다 22
force-group 공유 설정을 사용하여 ONTAP SMB 사용자 액세스를 최적화합니다 25
강제 그룹 공유 설정을 사용하여 ONTAP SMB 공유를 생성합니다 26
MMC를 사용하여 ONTAP SMB 공유에 대한 정보를 봅니다 26
SMB 공유를 관리하기 위한 ONTAP 명령 28
SMB 공유 ACL을 사용하여 파일 액세스 보호 28
ONTAP SMB 공유 레벨 ACL 관리에 대해 자세히 알아보십시오 28

ONTAP SMB 공유 액세스 제어 목록을 생성합니다 29
SMB 공유 액세스 제어 목록을 관리하기 위한 ONTAP 명령 31
파일 권한을 사용하여 파일 액세스를 보호합니다 32
ONTAP SMB SVM에 대한 Windows 보안 탭을 사용하여 고급 NTFS 파일 권한 구성 32
SMB NTFS 파일 권한에 대한 ONTAP 명령 35
ONTAP SMB 서버를 통해 파일에 액세스할 때 액세스 제어를 제공하는 UNIX 파일 권한에 대해 알아보세요. 35
DAC(Dynamic Access Control)를 사용하여 파일 액세스 보안 36
ONTAP SMB 서버에 대한 DAC 파일 액세스 보안에 대해 알아보세요 36
ONTAP SMB 서버에 지원되는 DAC 기능 37
ONTAP SMB 서버에서 DAC 및 중앙 액세스 정책을 사용하는 방법에 대해 알아보세요. 38
ONTAP SMB 서버에 대한 DAC 활성화 또는 비활성화 39
ONTAP SMB 서버에서 DAC가 비활성화된 경우 DAC ACE가 포함된 ACL 관리 40
ONTAP SMB 서버의 데이터를 보호하기 위한 중앙 액세스 정책 구성 40
ONTAP SMB 서버의 DAC 보안에 대한 정보 표시 43
ONTAP SMB 서버의 DAC에 대한 고려 사항 되돌리기 44
내보내기 정책을 사용하여 SMB 액세스를 보호합니다 45
ONTAP SMB 액세스를 통한 내보내기 정책 사용에 대해 알아보세요 45
ONTAP SMB 수출 규칙에 대해 알아보세요 46
SMB를 통한 액세스를 제한하거나 허용하는 ONTAP 내보내기 정책 규칙의 예 47
SMB 액세스를 위한 ONTAP 내보내기 정책 활성화 또는 비활성화 49
Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다 50
Storage-Level Access Guard를 사용하여 안전한 ONTAP SMB 파일 액세스에 대해 알아보세요. 50
Storage-Level Access Guard 사용 사례 51
ONTAP SMB 서버에서 Storage-Level Access Guard에 대한 구성 워크플로 52
ONTAP SMB 서버에서 스토리지 수준 액세스 보호 구성 54
ONTAP SMB 서버의 효과적인 SLAG 매트릭스 59
ONTAP SMB 서버에서 Storage-Level Access Guard에 대한 정보 표시 59
ONTAP SMB 서버에서 스토리지 수준 액세스 보호 제거 62

SMB를 사용하여 파일 액세스를 설정합니다

보안 스타일을 구성합니다

보안 스타일이 데이터 액세스에 미치는 영향

ONTAP SMB 보안 스타일과 그 영향에 대해 알아보십시오

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		
NTFS입니다	중소기업	NTFS ACL	NTFS입니다	
혼합	NFS 또는 SMB	NFSv3 모드 비트	Unix	
		NFSv4.ACL		
		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	NTFS입니다	

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.

그만큼 `show-effective-permissions` 매개변수를 사용하여 `vserver security file-directory` 명령을 사용하면 지정된 파일이나 폴더 경로에 대해 Windows 또는 UNIX 사용자에게 부여된 유효 권한을 표시할 수 있습니다. 또한 선택적 매개 변수를 `-share-name` 사용하면 효과적인 공유 권한을 표시할 수 있습니다. 에 대한 자세한

내용은 `vserver security file-directory show-effective-permissions` "ONTAP 명령 참조입니다"을 참조하십시오.

> 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.

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP SMB 보안 스타일을 설정할 위치 및 시기에 대해 알아보십시오

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.

ONTAP SVM에서 사용할 **SMB** 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	• 파일 시스템은 UNIX 관리자가 관리합니다. • 대부분의 사용자는 NFS 클라이언트입니다. • 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다.
NTFS입니다	• 파일 시스템은 Windows 관리자가 관리합니다. • 대부분의 사용자는 SMB 클라이언트입니다. • 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다.
혼합	파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다.

ONTAP SMB 보안 스타일 상속에 대해 알아보십시오

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.

ONTAP SMB FlexVol 볼륨에 대한 **UNIX** 사용 권한을 유지하는 방법에 대해 알아봅니다

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.

ONTAP SMB 서버의 **Windows** 보안 탭을 사용하여 **UNIX** 권한을 관리하는 방법에 대해 알아봅니다

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.

ONTAP SVM 루트 볼륨에 SMB 보안 형식을 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 혼합 입니다.

2. 생성한 SVM의 루트 볼륨 보안 스타일('vserver show -vserver_vserver_name_')을 포함하여 구성을 표시하고 확인합니다

ONTAP FlexVol 볼륨에 SMB 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 혼합 입니다.

   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'

ONTAP qtree에서 SMB 보안 스타일을 구성합니다

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, 혼합 입니다.

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 ONTAP SMB 데이터 볼륨을 생성하고 관리하는 방법에 대해 알아보십시오

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 접합 지점으로 ONTAP SMB 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 /eng은 /eng과 같습니다. CIFS 공유를 생성하는 경우 Windows는 연결 경로를 대/소문자를 구분하는 것처럼 처리합니다. 예를 들어, junction이 /eng인 경우 CIFS 공유의 경로는 /eng가 아니라 /eng로 시작해야 합니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 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
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

접합 지점을 지정하지 않고 **ONTAP SMB** 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. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 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
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NAS 네임스페이스에서 기존 ONTAP SMB 볼륨을 마운트하거나 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 엑스포트 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_'

볼륨을 마운트 해제합니다	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

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
```

ONTAP SMB 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	a. 필요한 경우 볼륨 표시 필드? 명령을 사용하여 '-fields' 매개 변수에 대한 유효한 필드를 표시할 수 있습니다 b. '-fields' 매개 변수를 사용하여 원하는 정보를 표시합니다. volume show -vserver vserver_name -fields fieldname,…

예

다음 예는 SVM VS1 에서 마운트 및 마운트 해제된 볼륨에 대한 요약을 표시합니다.

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   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

ONTAP SMB 이름 매핑 구성에 대해 자세히 알아보십시오

ONTAP는 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 증명이 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.

ONTAP SMB 이름 매핑에 대해 자세히 알아보십시오

ONTAP에서 사용자에 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.

UNIX 사용자와 Windows 사용자 이름 간 매핑에 대한 ONTAP SMB 다중 도메인 검색에 대해 알아봅니다

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_sunfre검색되었습니다.

- _ 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_sound입니다.

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.
*	\ * \\ *	유효한 UNIX 사용자는 해당 Windows 사용자에게 매핑됩니다. 모든 신뢰할 수 있는 도메인은 해당 이름을 가진 첫 번째 일치하는 사용자를 찾을 때까지 순서대로 검색됩니다. 패턴 \ * \\ * 은 UNIX에서 Windows로의 이름 매핑에만 유효하며 다른 방법은 사용할 수 없습니다.

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.

ONTAP SMB 이름 매핑 변환 규칙에 대해 알아보십시오

ONTAP 시스템은 각 SVM에 대해 일련의 전환 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.

ONTAP SMB 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 이 문을 사용하여 `null` 대체 문자열(공백 문자)을 사용하여 사용자에 대한 매핑을 명시적으로 거부할 `" "` 수도 `-replacement` 있습니다. 에 대한 자세한 내용은 `vserver name-mapping create` link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["ONTAP 명령 참조입니다"^]을 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\JohnnDoe에 매핑합니다.

```
vs1::> vserver name-mapping create -vserver 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::> vserver name-mapping create -vserver 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::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

기본 **ONTAP SMB** 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	'vserver cifs options modify-default-unix-user_user_name_'

원하는 작업	다음 명령을 입력합니다...
기본 Windows 사용자를 구성합니다	'vserver nfs modify -default-win-user_user_name_'

SMB 이름 매핑을 관리하기 위한 ONTAP 명령

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. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	`vserver name-mapping swap`
이름 매핑을 수정합니다	`vserver name-mapping modify`
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`

에 대한 자세한 내용은 `vserver name-mapping` "ONTAP 명령 참조입니다"을 참조하십시오.

다중 도메인 이름 매핑 검색을 구성합니다

ONTAP SMB 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 서버 옵션

신뢰할 수 있는 ONTAP SMB 도메인을 재설정하고 재검색합니다

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 정보를 표시합니다

검색된 신뢰할 수 있는 ONTAP SMB 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 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 도메인을 다시 설정하고 다시 검색합니다

기본 설정 목록에서 신뢰할 수 있는 **ONTAP SMB** 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

기본 설정 신뢰할 수 있는 도메인 목록에 대한 정보를 표시합니다

기본 설정 신뢰할 수 있는 ONTAP SMB 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

선호하는 목록에서 신뢰할 수 있는 도메인을 추가, 제거 또는 교체합니다.

SMB 공유를 생성하고 구성합니다

ONTAP SMB 공유 생성 및 구성에 대해 자세히 알아보십시오

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 ONTAP는 모든 사용자에 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

- 로컬 사용자 및 그룹에 대해 알아보세요
- "Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"

- 볼륨에서 파일 이름 번역을 위한 문자 매핑 구성

기본 관리 **ONTAP SMB** 공유에 대해 알아봅니다

SVM(스토리지 가상 시스템)에서 CIFS 서버를 생성하면 기본 관리 공유가 자동으로 생성됩니다. 이러한 기본 공유가 무엇이고 어떻게 사용되는지 이해해야 합니다.

ONTAP는 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.

관련 정보

Windows 보안 탭을 사용하여 고급 파일 권한 구성

ONTAP SMB 공유 명명 요구사항에 대해 알아보십시오

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$을(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.

```
** [ ] " / \ : ; | < > , ? * =
```

멀티 프로토콜 환경에서 공유를 생성할 때의 **ONTAP SMB** 디렉토리 대소문자 구분 요구사항에 대해 알아보십시오

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 `/home'입니다. 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

ONTAP SMB 공유 속성 사용에 대해 자세히 알아보십시오

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 스냅샷을 보고 탐색할 수 있도록 지정합니다.

공유 속성	설명
'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.
"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 디렉토리 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 **ONTAP 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:

- 쉼표로 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::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path      Properties   Comment    ACL
---------  ------   --------  ----------   --------   -----------
vs1        share2   /share2   oplocks      -          Everyone / Full
Control
                              changenotify
```

관련 정보

공유 관리를 위한 명령

force-group 공유 설정을 사용하여 ONTAP 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-group을 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-group이 지정된 경우 공유의 다음 내용이 적용됩니다.

- 이 공유에 액세스하는 force-group의 SMB 사용자는 force-group의 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-group은 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-group을 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

강제 그룹 공유 설정으로 공유 만들기

강제 그룹 공유 설정을 사용하여 **ONTAP 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

강제 그룹 공유 설정을 사용하여 사용자 액세스 최적화

MMC를 사용하여 **ONTAP 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 관리하기 위한 ONTAP 명령

'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

에 대한 자세한 내용은 `vserver cifs` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 공유 ACL을 사용하여 파일 액세스 보호

ONTAP SMB 공유 레벨 ACL 관리에 대해 자세히 알아보십시오

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.

기본적으로 공유 수준 ACL은 Everyone이라는 표준 그룹에 모든 권한을 부여합니다. ACL에 대한 모든 제어 기능은 도메인 및 모든 신뢰할 수 있는 도메인의 모든 사용자가 공유에 대한 모든 액세스 권한을 갖는다는 것을 의미합니다. Windows 클라이언트의 Microsoft Management Console(MMC)이나 ONTAP 명령줄을 사용하여 공유 수준 ACL에 대한 액세스 수준을 제어할 수 있습니다. "공유 액세스 제어 목록 만들기"..

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.

ONTAP 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 ACL인 'vserver cifs share access-control delete-vserver <vserver_name>-share <share_name>-user-or-group everyone'을 삭제하십시오
2. 새 ACL 구성:

을 사용하여 **ACL**을 구성하려면…	명령 입력…
Windows 사용자	`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>`
Windows 그룹	`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>`

을 사용하여 **ACL**을 구성하려면...	명령 입력...
Unix 사용자입니다	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
Unix 그룹	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

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

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

다음 명령을 실행하면 `Read` "vs2.example.com" SVM의 "eng" 공유에 대한 "engineering" UNIX 그룹에 대한 권한이 부여됩니다.

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

다음 명령은 `Change` "Tiger Team"이라는 로컬 Windows 그룹에 `Full_Control` 대한 권한을 부여하고 "VS1" SVM에서 "datavol5" 공유에 대해 "Sue Chang"이라는 로컬 Windows 사용자에게 권한을 부여합니다.

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

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

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
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 관리하기 위한 ONTAP 명령

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	'vserver cifs share access-control create'
ACL을 표시합니다	'vserver cifs share access-control show'를 참조하십시오
ACL을 수정합니다	'vserver cifs share access-control modify'를 참조하십시오
ACL을 삭제한다	'vserver cifs share access-control delete'

파일 권한을 사용하여 파일 액세스를 보호합니다

ONTAP SMB SVM에 대한 **Windows** 보안 탭을 사용하여 고급 **NTFS** 파일 권한 구성

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	a. 추가 * 를 클릭합니다. b. 선택할 개체 이름 입력 * 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다. c. 확인 * 을 클릭합니다.
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 건너뜁니다.

   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

- 서버에 NTFS 보안 설명자 만들기
- NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다
- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

SMB NTFS 파일 권한에 대한 ONTAP 명령

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 디렉터리에 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
   ```

ONTAP SMB 서버를 통해 파일에 액세스할 때 액세스 제어를 제공하는 UNIX 파일 권한에 대해 알아보세요.

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

ONTAP SMB 서버에 대한 DAC 파일 액세스 보안에 대해 알아보세요

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 멤버쉽은 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 GPO에 대해 알아보세요
- SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.
- 서버에서 GPO 지원 활성화 또는 비활성화
- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다
- 서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다.
- 서버 보안에 대한 정보 표시
- "SMB 및 NFS 감사 및 보안 추적"

ONTAP SMB 서버에 지원되는 DAC 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 사용자에 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.

기능	설명
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.
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.

ONTAP SMB 서버에서 **DAC** 및 중앙 액세스 정책을 사용하는 방법에 대해 알아보세요**.**

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 Directory에서 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.

ONTAP SMB 서버에 대한 DAC 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.

Active Directory에서 동적 액세스 제어를 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

"Microsoft TechNet: 동적 액세스 제어 시나리오 개요"

이 작업에 대해

동적 액세스 제어가 설정되면 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

서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다.

ONTAP SMB 서버에서 DAC가 비활성화된 경우 DAC ACE가 포함된 ACL 관리

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.

ONTAP SMB 서버의 데이터를 보호하기 위한 중앙 액세스 정책 구성

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. Active Directory의 중앙 액세스 정책을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

"Microsoft TechNet: 중앙 액세스 정책 시나리오"

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/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

  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

- SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.
- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다
- 서버에 대한 DAC 활성화 또는 비활성화

ONTAP SMB 서버의 DAC 보안에 대한 정보 표시

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 디렉토리 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 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

ONTAP SMB 서버의 DAC에 대한 고려 사항 되돌리기

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.

내보내기 정책을 사용하여 **SMB** 액세스를 보호합니다

ONTAP SMB 액세스를 통한 내보내기 정책 사용에 대해 알아보세요

SMB 서버에서 SMB 액세스에 대한 엑스포트 정책을 사용하는 경우, SMB 클라이언트에서 SVM 볼륨에 대한 액세스를 제어할 때 엑스포트 정책이 사용됩니다. 데이터에 액세스하려면 SMB 액세스를 허용하는 엑스포트 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 엑스포트 정책을 연결합니다. 각 SVM에는 여러 엑스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨이 있는 SVM에 대해 다음을 수행할 수 있습니다.

- SVM의 각 볼륨에 서로 다른 엑스포트 정책을 지정하여 개별 클라이언트 액세스 제어를 SVM의 각 볼륨에 할당

- 각 볼륨에 대해 새로운 엑스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨에 동일한 엑스포트 정책을 할당합니다.

각 SVM에는 규칙이 없는 "기본값"이라는 엑스포트 정책이 하나 이상 있습니다. 이 엑스포트 정책을 삭제할 수는 없지만 이름을 바꾸거나 수정할 수는 있습니다. 기본적으로 SVM의 각 볼륨은 기본 엑스포트 정책과 연결됩니다. SVM에서 SMB 액세스에 대한 엑스포트 정책을 사용하지 않도록 설정한 경우, "기본값" 엑스포트 정책은 SMB 액세스에 영향을 미치지 않습니다.

NFS 및 SMB 호스트 모두에 대한 액세스를 제공하는 규칙을 구성하고 이 규칙을 엑스포트 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 엑스포트 정책을 구성할 수 있습니다. 그러면 엑스포트 정책이 SMB 액세스만 원하는 볼륨에 연결됩니다.

SMB에 대한 엑스포트 정책이 설정되어 있고 클라이언트가 해당 엑스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우, 요청이 실패하고 권한 거부 메시지가 표시됩니다. 클라이언트가 볼륨의 엑스포트 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 엑스포트 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".

ONTAP SMB 수출 규칙에 대해 알아보세요

내보내기 규칙은 엑스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을 처리하는 방법을 결정하기 위해 구성한 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청을 일치시킵니다.

클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 엑스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 엑스포트 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

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 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

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 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

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 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.

SMB를 통한 액세스를 제한하거나 허용하는 **ONTAP** 내보내기 정책 규칙의 예

이 예에서는 SMB 액세스에 대한 엑스포트 정책이 설정된 SVM에서 SMB를 통한 액세스를 제한 또는 허용하는 엑스포트 정책 규칙을 생성하는 방법을 보여줍니다.

SMB 액세스에 대한 엑스포트 정책은 기본적으로 비활성화되어 있습니다. SMB 액세스에 대한 엑스포트 정책을 설정한 경우에만 SMB 액세스를 제한하거나 허용하는 엑스포트 정책 규칙을 구성해야 합니다.

SMB 액세스에 대한 엑스포트 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 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 엑스포트 규칙

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 규칙이 생성됩니다.

- 정책 이름: cifsnfs1
- 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::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

NTLM을 사용한 **SMB** 액세스에 대한 내보내기 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 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::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

SMB 액세스를 위한 ONTAP 내보내기 정책 활성화 또는 비활성화

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 엑스포트 정책을 설정하거나 해제할 수 있습니다. 내보내기 정책을 사용하여 리소스에 대한 SMB 액세스를 제어하는 것은 선택 사항입니다.

시작하기 전에

다음은 SMB에 대한 엑스포트 정책을 설정하기 위한 요구 사항입니다.

- 클라이언트에 대한 내보내기 규칙을 만들기 전에 DNS에 "PTR" 레코드가 있어야 합니다.
- SVM에서 NFS 클라이언트에 대한 액세스를 제공하고 NFS 액세스에 사용할 호스트 이름이 CIFS 서버 이름과 다른 경우 호스트 이름에 대한 추가 "A" 및 "PTR" 레코드 세트가 필요합니다.

이 작업에 대해

SVM에서 새 CIFS 서버를 설정할 때 SMB 액세스에 대한 엑스포트 정책을 사용하는 것은 기본적으로 해제되어 있습니다. 인증 프로토콜 또는 클라이언트 IP 주소 또는 호스트 이름을 기반으로 액세스를 제어하려는 경우 SMB 액세스에 대한 엑스포트 정책을 설정할 수 있습니다. 언제든지 SMB 액세스에 대한 엑스포트 정책을 설정하거나 해제할 수 있습니다.

NFS 지원 SVM에서 CIFS/SMB에 대한 엑스포트 정책을 활성화하면 Linux 클라이언트가 SVM에서 명령을 사용하여 연결된 엑스포트 정책 규칙을 통해 모든 SMB 볼륨의 접합 경로를 볼 수 있습니다 `showmount -e`.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 엑스포트 정책 활성화 또는 비활성화:
   - 내보내기 정책 활성화: 'vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled true'
   - 엑스포트 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 엑스포트 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 안전한 ONTAP SMB 파일 액세스에 대해 알아보세요.

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 사용자에 대한 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 디렉터리에만 적용하거나 볼륨 내의 파일과 디렉터리에 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 디렉터리에 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 접합 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.

액세스 확인 순서

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 디렉터리에 있는 유효한 권한을 결정합니다. 보안 액세스 검사는 다음 순서로 수행됩니다.

1. SMB 공유 또는 NFS 엑스포트 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

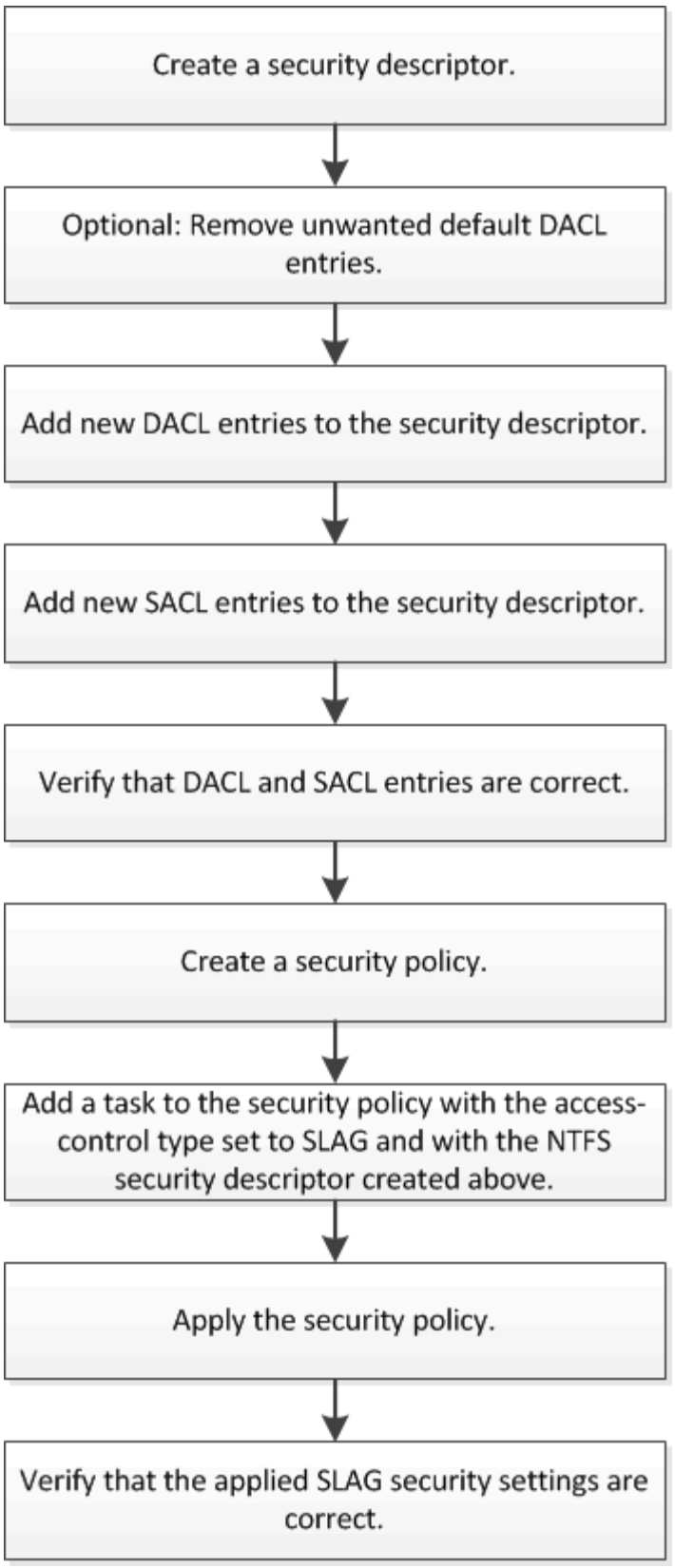
Storage-Level Access Guard는 클라이언트 측에서 볼 수 없는 스토리지 수준에서 추가 보안을 제공하므로 사용자 또는 관리자가 데스크톱에서 해당 보안을 취소할 수 없습니다. 스토리지 레벨에서 액세스를 제어하는 기능이 유용하다고 볼 수 있는 특정 사용 사례가 있습니다.

이 기능의 일반적인 사용 사례는 다음과 같습니다.

- 스토리지 수준에서 모든 사용자의 액세스를 감사 및 제어하여 지적 재산권을 보호합니다
- 은행 및 거래 그룹을 비롯한 금융 서비스 기업을 위한 스토리지
- 정부 서비스 및 개별 부서용 개별 파일 스토리지
- 모든 학생 파일을 보호하는 대학

ONTAP SMB 서버에서 **Storage-Level Access Guard**에 대한 구성 워크플로

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

서버에서 스토리지 수준 액세스 보호 구성

ONTAP SMB 서버에서 스토리지 수준 액세스 보호 구성

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    Owner Name
   Descriptor 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   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    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   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    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   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    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   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    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 디렉토리 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

- NTFS 파일 보안, NTFS 감사 정책 및 스토리지 수준 액세스 보호 관리를 위한 명령
- 서버의 Storage-Level Access Guard에 대한 구성 워크플로
- 서버의 Storage-Level Access Guard에 대한 정보 표시
- 서버에서 스토리지 수준 액세스 보호 제거

ONTAP SMB 서버의 효과적인 SLAG 매트릭스

볼륨 또는 qtree 또는 둘 다에서 슬래그를 구성할 수 있습니다. 슬래그 매트릭스는 표에 나열된 다양한 시나리오에서 적용 가능한 슬래그 구성인 볼륨 또는 qtree를 정의합니다.

	AFS에서 볼륨 슬래그	스냅샷의 볼륨 슬래그	**AFS**에서 **qtree** 슬래그	스냅샷에서 **Qtree** 슬래그
AFS(Access File System)에서 볼륨 액세스	예	아니요	해당 없음	해당 없음
스냅샷의 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
스냅샷에서 qtree 액세스(qtree AFS에 슬래그가 있는 경우)	아니요	아니요	예	아니요
스냅샷에서 qtree 액세스(qtree AFS에 슬래그가 없는 경우)	예	아니요	아니요	아니요

ONTAP SMB 서버에서 Storage-Level Access Guard에 대한 정보 표시

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
```

ONTAP SMB 서버에서 스토리지 수준 액세스 보호 제거

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
```