SMB를 사용하여 파일 액세스를 관리합니다
ONTAP 9

NetApp
February 12, 2026

목차

SMB를 사용하여 파일 액세스를 관리합니다

로컬 사용자 및 그룹을 인증 및 인증에 사용합니다

ONTAP에서 로컬 사용자 및 그룹을 사용하는 방법

로컬 **ONTAP SMB** 사용자 및 그룹에 대해 알아보세요

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 **ONTAP SMB** 사용자 및 로컬 그룹을 생성하는 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 사용자에 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 인증에 대해 알아보세요
- 지원되는 권한 목록입니다

로컬 **ONTAP SMB** 사용자 인증에 대해 알아보세요

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.

ONTAP는 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

  ONTAP는 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 ONTAP는 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 ONTAP는 CIFS 서버에서 해당 로컬 계정을 사용하여 인증합니다.

- 도메인 부분이 지정되지 않았습니다

  ONTAP는 먼저 로컬 사용자로 인증을 시도합니다. 로컬 사용자로 인증에 실패하면 ONTAP는 CIFS 서버가 속한 도메인의 도메인 컨트롤러를 사용하여 사용자를 인증합니다.

로컬 또는 도메인 사용자 인증이 성공적으로 완료되면 ONTAP는 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

서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다.

ONTAP SMB 사용자 액세스 토큰에 대해 알아보세요

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 **ONTAP SMB SVM**에서 **SnapMirror**를 사용하는 방법에 대해 알아보세요**.**

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.

ONTAP SMB 서버를 삭제하면 사용자와 그룹에 어떤 영향이 있는지 알아보세요**.**

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 **ONTAP SMB** 사용자 및 그룹과 함께 **Microsoft Management Console**을 사용하는 방법을 알아보세요**.**

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.

ONTAP SMB 클러스터 되돌리기에 대해 알아보세요

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 **ONTAP SMB** 권한 목록

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
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

- 권한 할당에 대해 알아보세요
- 바이패스 트래버스 검사 구성에 대해 알아보세요

ONTAP SMB 권한 할당에 대해 알아보세요

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 권한을 추가합니다
- 로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거합니다
- 로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정합니다
- 바이패스 트래버스 검사 구성에 대해 알아보세요

ONTAP SMB 서버의 **BUILTIN** 그룹 및 로컬 관리자 계정에 대해 알아보세요.

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 **ONTAP SMB** 사용자 암호에 대한 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:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

관련 정보

- 로컬 사용자에 대한 암호 복잡성 구성
- 서버 보안 설정에 대한 정보 표시
- 로컬 사용자 계정 암호를 변경합니다

미리 정의된 **BUILTIN** 그룹 및 기본 **ONTAP SMB** 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 **BUILTIN** 그룹	기본 권한
"BUILTIN\Administrators" RID 544 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.	• 'BackupPrivilege'입니다 • 스저장창고특권 • '보안 권한' • '새테이크오너선프리빌리지' • '스변경NotifyPrivilege'입니다
"BUILTIN\Power Users" RID 547 이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 다음과 같은 특성을 갖습니다. • 로컬 사용자 및 그룹을 생성하고 관리할 수 있습니다. • 자체 또는 다른 개체를 'BUILTIN\Administrators' 그룹에 추가할 수 없습니다.	'스변경NotifyPrivilege'입니다
``BUILTIN\Backup Operators' RID 551 이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 백업 의도로 열린 파일 또는 폴더에 대한 읽기 및 쓰기 권한을 재정의할 수 있습니다.	• 'BackupPrivilege'입니다 • 스저장창고특권 • '스변경NotifyPrivilege'입니다

미리 정의된 **BUILTIN** 그룹	기본 권한
"BUILTIN\Users" RID 545 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.	'스변경NotifyPrivilege'입니다
모든 사람의 ID S-1-0입니다 이 그룹에는 게스트(익명 사용자 제외)를 포함한 모든 사용자가 포함됩니다. 이 그룹은 묵시적 멤버십을 가진 암시적 그룹입니다.	'스변경NotifyPrivilege'입니다

관련 정보

- 서버의 BUILTIN 그룹 및 로컬 관리자 계정에 대해 알아보세요.
- 지원되는 권한 목록입니다
- 바이패스 트래버스 검사 구성에 대해 알아보세요

로컬 사용자 및 그룹 기능을 설정하거나 해제합니다

로컬 **ONTAP SMB** 사용자 및 그룹 기능에 대해 알아보세요

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

ONTAP SMB 서버에서 로컬 사용자 및 그룹 활성화 또는 비활성화

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::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

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

관련 정보

- 서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다.
- 로컬 사용자 계정을 설정하거나 해제합니다

ONTAP SMB 서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다**.**

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	'vserver cifs options modify -vserver_vserver_name_-is-local-auth-enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_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::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

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

관련 정보

- 로컬 사용자 인증에 대해 알아보세요
- 서버에서 로컬 사용자 및 그룹 활성화 또는 비활성화

로컬 사용자 계정을 관리합니다

로컬 **ONTAP SMB** 사용자 계정 수정

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	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -full-name text' 전체 이름에 공백이 포함되어 있으면 큰따옴표로 묶어야 합니다.
로컬 사용자의 설명을 수정합니다	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -description text' 설명에 공백이 포함된 경우 큰따옴표로 묶어야 합니다.
로컬 사용자 계정을 활성화하거나 비활성화합니다	'vserver cifs users-and-groups local-user modify -vserver_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::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

로컬 **ONTAP SMB** 사용자 계정 활성화 또는 비활성화

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	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -is-account-disabled false'
사용자 계정을 비활성화합니다	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -is-account-disabled true'

로컬 **ONTAP SMB** 사용자 계정 비밀번호 변경

로컬 사용자의 계정 암호를 변경할 수 있습니다. 이 방법은 사용자의 암호가 손상되었거나 사용자가 암호를 잊어버린 경우에 유용합니다.

단계

1. 'vserver cifs users-and-groups local-user set-password-vserver_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::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

관련 정보

로컬 사용자에 대한 암호 복잡성 구성

서버 보안 설정에 대한 정보 표시

ONTAP SMB 로컬 사용자에 대한 정보 표시

모든 로컬 사용자의 목록을 요약 양식에 표시할 수 있습니다. 특정 사용자에 대해 구성된 계정 설정을 확인하려면 해당 사용자에 대한 자세한 계정 정보와 여러 사용자에 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 사용자에 대한 정보 표시	'vserver cifs users-and-groups local-user show -vserver_vserver_name_'
사용자에 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. 에 대한 자세한 내용은 `vserver cifs`

"ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예제는 SVM VS1 의 모든 로컬 사용자에 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 **ONTAP SMB** 그룹 멤버십에 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::> vserver 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 **ONTAP SMB** 사용자 계정 삭제

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 **ONTAP SMB** 그룹 수정

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::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

다음 예에서는 로컬 그룹 ""cifs_server\engineering""의 설명을 수정합니다.

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

ONTAP SMB 로컬 그룹에 대한 정보 표시

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	'vserver cifs users-and-groups local-group show'를 참조하십시오
SVM의 모든 로컬 그룹	'vserver cifs users-and-groups local-group show -vserver_vserver_name_'

이 명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예제는 SVM VS1 의 모든 로컬 그룹에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs users-and-groups local-group show -vserver 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 ONTAP SMB 그룹 구성원 자격을 관리합니다

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 구성원 자격을 관리할 수 있습니다. 이 기능은 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하려는 경우 또는 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 쉼표로 구분된 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 목록을 지정할 수 있습니다.
그룹에서 구성원을 제거합니다	'vserver cifs users-and-groups local-group remove-memers-vserver_name_-group-name_group_name_-member-names name[,...]'지정된 로컬 그룹에서 제거할 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 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 정보를 표시합니다

로컬 그룹 구성원에 대한 **ONTAP SMB** 정보 표시

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::> vserver 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 **ONTAP SMB** 그룹 삭제

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. 'vserver cifs users-and-groups local-group show -vserver vserver_name'
2. 로컬 그룹 'vserver cifs users-and-groups local-group delete -vserver_vserver_name_-group-name_group_name_'을 삭제합니다
3. 그룹이 삭제되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 관련 로컬 그룹 ""cifs_server\sales""를 삭제합니다.

```
cluster1::> vserver cifs users-and-groups local-group show -vserver 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::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver 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 **ONTAP SMB** 도메인 사용자 및 그룹 이름 업데이트

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	'vserver cifs users-and-groups update-names-vserver_vserver_name_'
성공적으로 업데이트된 도메인 사용자 및 그룹을 표시합니다	'vserver cifs users-and-groups update-names-vserver_vserver_name_-display-failed-only false'
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::*> vserver cifs users-and-groups update-names -vserver 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

ONTAP SMB 로컬 또는 도메인 사용자나 그룹에 권한 추가

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 ONTAP는 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
```

ONTAP SMB 로컬 또는 도메인 사용자나 그룹의 권한 제거

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 ONTAP는 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       -
```

ONTAP SMB 로컬 또는 도메인 사용자 및 그룹에 대한 권한 재설정

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.
```

ONTAP SMB 권한 재정의에 대한 정보 표시

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. 에 대한 자세한 내용은 `vserver cifs users-and-groups privilege show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령을 실행하면 SVM VS1 에 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

ONTAP SMB 바이패스 트래버스 검사 구성에 대해 알아보세요.

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 사용자에 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 디렉토리에 대한 통과 권한을 확인하지 않습니다.
- 허용되지 않는 경우 ONTAP는 파일 경로에 있는 모든 디렉토리에 대해 트래버스(실행) 권한을 확인합니다.

  중간 디렉토리에 ""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 파일 이름 번역을 위한 문자 매핑 구성
- 공유 액세스 제어 목록 만들기
- Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다
- 지원되는 권한 목록입니다
- 로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다

사용자 또는 그룹이 **ONTAP SMB** 디렉터리 트래버스 검사를 우회하도록 허용

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 ONTAP는 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

디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다

사용자 또는 그룹이 **ONTAP SMB** 디렉터리 트래버스 검사를 우회하는 것을 허용하지 않음

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 ONTAP는 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 건너뛰도록 허용합니다

파일 보안 및 감사 정책에 대한 정보를 표시합니다

ONTAP SMB 파일 보안 및 감사 정책 보기에 대해 알아보세요

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 안전한 파일 액세스에 대해 알아보세요
- 서버의 Storage-Level Access Guard에 대한 정보 표시

NTFS 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시

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
                             .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

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
```

```
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
```

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 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

혼합 보안 스타일 볼륨에서 **ONTAP SMB** 파일 보안에 대한 정보 표시

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 디렉토리 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 디렉토리의 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 디렉토리 경로에 동적 액세스 제어가 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 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

UNIX 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시

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: -
```

관련 정보

- 보안 스타일 볼륨의 파일 보안에 대한 정보 표시
- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다

SMB FlexVol 볼륨의 NTFS 감사 정책에 대한 정보를 표시하는 ONTAP 명령

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 제어가 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
```

SMB FlexVol 볼륨의 NFSv4 감사 정책에 대한 정보를 표시하는 ONTAP 명령

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
```

ONTAP SMB 파일 보안 및 감사 정책 정보를 표시하는 방법을 알아보세요.

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 디렉터리의 정보를 표시할 아래의 지정된 디렉터리 경로의 마지막 하위 구성 요소로 사용할 수 있습니다. "" * ""로 명명된 특정 파일이나 디렉터리의 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::> vserver security file-directory show -vserver 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

SMB NTFS 파일 보안, NTFS 감사 정책 및 스토리지 수준 액세스 보호 관리를 위한 ONTAP 명령

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, ONTAP는 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 정책 보기에 대해 알아보세요
- 서버에 NTFS 보안 설명자 만들기
- 파일 및 폴더에 감사 정책을 구성하고 적용하는 명령
- Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요

SMB 파일 및 폴더 보안을 설정하기 위한 **ONTAP** 명령

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

ONTAP 명령을 사용하여 SMB 파일 및 폴더 보안을 설정할 때의 제한 사항에 대해 알아보세요.

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 ONTAP SMB 파일 및 폴더 보안을 적용합니다.

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"
- 파일 및 폴더에 감사 정책을 구성하고 적용하는 명령

ONTAP SVM 재해 복구 대상에서 로컬 SMB 사용자 또는 그룹을 사용하는 파일 디렉토리 정책을 적용하는 방법에 대해 알아보세요.

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""""로 자동 변경됩니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      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('vserver 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::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **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.

CLI를 사용하여 NTFS 파일 및 폴더에 파일 보안을 구성하고 적용합니다

ONTAP SMB 서버에서 NTFS 보안 설명자 생성

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 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP SMB 서버의 **NTFS** 보안 설명자에 **NTFS DACL** 액세스 제어 항목 추가

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. 이 절차에서 설명하는 명령에 대한 자세한

내용은 를 "ONTAP 명령 참조입니다"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_SIDoptional_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
```

에 대한 자세한 내용은 `vserver security file-directory ntfs dacl` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SMB 보안 정책 생성

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
```

ONTAP SMB 보안 정책에 작업 추가

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 디렉토리 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. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉토리 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
```

에 대한 자세한 내용은 `vserver security file-directory policy task` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SMB 보안 정책 적용

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
   ```

ONTAP SMB 보안 정책 작업 모니터링

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
   ```

ONTAP SMB 파일 보안 확인

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

                            ALLOW-Everyone-0x10000000-OI|CI|IO
```

```
                                0... .... .... .... .... .... .... .... =
Generic Read
                                .0.. .... .... .... .... .... .... .... =
Generic Write
                                ..0. .... .... .... .... .... .... .... =
Generic Execute
                                ...1 .... .... .... .... .... .... .... =
Generic All
                                .... ...0 .... .... .... .... .... .... =
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
```

CLI를 사용하여 NTFS 파일 및 폴더에 감사 정책을 구성하고 적용합니다

NTFS 파일 및 폴더에 SMB 감사 정책을 구성하고 적용하기 위한 ONTAP 명령

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 안전한 파일 액세스에 대해 알아보세요
- SMB 파일 및 폴더 보안을 설정하기 위해 명령을 사용할 때의 제한 사항에 대해 알아보세요.
- 보안 설명자를 사용하여 파일 및 폴더 보안을 적용합니다.
- "SMB 및 NFS 감사 및 보안 추적"
- 서버에 NTFS 보안 설명자 만들기

ONTAP SMB 서버에서 **NTFS** 보안 설명자 생성

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. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"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 vserver_name-NTFS-SD 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 vserver_name -NTFS-SD sd_name'

   ```
   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

ONTAP SMB 서버의 **NTFS** 보안 설명자에 **NTFS SACL** 액세스 제어 항목 추가

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 vserver_name -ntfs -sd sd sd_name -access -type {failure | success} -account name_or_SIDoptional_parameters'

   'vserver security file-directory NTFS SACL add-NTFS-SD SD1-access-type failure-account domain\joe-rights full-control-apply-to this-folder-vserver-vs1'

2. SACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS SACL show -vserver vserver_name -ntfs -sd sd sd_name -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
```

ONTAP SMB 보안 정책 생성

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
```

ONTAP SMB 보안 정책에 작업 추가

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 디렉토리 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. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉토리 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
```

에 대한 자세한 내용은 `vserver security file-directory policy task` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SMB 보안 정책 적용

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
```

ONTAP SMB 보안 정책 작업 모니터링

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
```

ONTAP SMB 감사 정책 확인

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
```

ONTAP SMB 보안 정책 작업 관리에 대해 알아보세요

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.

SMB 서버에서 NTFS 보안 설명자를 관리하기 위한 ONTAP 명령

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

에 대한 자세한 내용은 `vserver security file-directory ntfs` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 서버에서 NTFS DACL 액세스 제어 항목을 관리하기 위한 ONTAP 명령

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'

에 대한 자세한 내용은 `vserver security file-directory ntfs dacl` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 서버에서 NTFS SACL 액세스 제어 항목을 관리하기 위한 ONTAP 명령

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'

에 대한 자세한 내용은 `vserver security file-directory ntfs sacl` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 보안 정책을 관리하기 위한 ONTAP 명령

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

에 대한 자세한 내용은 `vserver security file-directory policy` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 보안 정책 작업을 관리하기 위한 ONTAP 명령

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'

원하는 작업	이 명령 사용...
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'

에 대한 자세한 내용은 `vserver security file-directory policy task` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 보안 정책 작업을 관리하기 위한 ONTAP 명령

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'

에 대한 자세한 내용은 `vserver security file-directory job` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 공유에 대한 메타데이터 캐시를 구성합니다

ONTAP SMB 메타데이터 캐싱에 대해 알아보세요

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 시간 을 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.

ONTAP SMB 메타데이터 캐시 활성화

SMB 메타데이터 캐시를 설정하여 SMB 1.0 클라이언트의 SMB 성능을 향상할 수 있습니다. 기본적으로 SMB 메타데이터 캐싱은 해제되어 있습니다.

단계

1. 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

- 메타데이터 캐시 항목의 수명 구성
- 기존 주식에 주식 속성 추가 또는 제거

ONTAP SMB 메타데이터 캐시 항목의 수명 구성

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

1. 원하는 작업을 수행합니다.

다음과 같은 경우 **SMB** 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]'

다음과 같은 경우 **SMB** 메타데이터 캐시 항목의 수명을 구성하려는 경우	명령 입력…
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. 에 대한 자세한 내용은 `vserver cifs share` "ONTAP 명령 참조입니다"을 참조하십시오.

파일 잠금 관리

프로토콜 간 **ONTAP SMB** 파일 잠금에 대해 알아보세요

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.

ONTAP SMB 읽기 전용 비트에 대해 알아보세요

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.

ONTAP는 Windows를 사용하는 SMB 클라이언트가 해당 파일을 생성할 때 파일에 읽기 전용 비트를 설정할 수 있습니다. 또한 ONTAP는 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 ONTAP는 해당 파일에 대해 읽기 전용 비트를 설정합니다.
- NFS 클라이언트가 쓰기 권한 비트를 설정하면 ONTAP는 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 ONTAP는 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 ONTAP는 해당 파일에 대한 소유자의 쓰기 권한 비트를 설정합니다.
- 읽기 전용 비트가 설정된 파일은 루트에서만 쓸 수 있습니다.

읽기 전용 비트는 다음과 같은 방식으로 ACL 및 Unix 모드 비트와 상호 작용합니다.

파일에 읽기 전용 비트가 설정된 경우:

- 해당 파일의 ACL에는 변경 사항이 없습니다. NFS 클라이언트는 읽기 전용 비트가 설정되기 전과 동일한 ACL을 보게 됩니다.
- 파일에 대한 쓰기 접근을 허용하는 모든 Unix 모드 비트는 무시됩니다.
- NFS와 SMB 클라이언트는 모두 파일을 읽을 수 있지만, 수정할 수는 없습니다.
- ACL 및 UNIX 모드 비트는 읽기 전용 비트 때문에 무시됩니다. 즉, ACL이 쓰기 액세스를 허용하더라도 읽기 전용 비트는 수정을 방지합니다.

파일에 읽기 전용 비트가 설정되지 않은 경우:

- ONTAP ACL 및 UNIX 모드 비트를 기반으로 액세스를 결정합니다.
  - ACL 또는 UNIX 모드 비트가 쓰기 액세스를 거부하는 경우 NFS 및 SMB 클라이언트는 파일을 수정할 수 없습니다.
  - ACL이나 UNIX 모드 비트가 쓰기 액세스를 거부하지 않으면 NFS 및 SMB 클라이언트가 파일을 수정할 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 요소에 대한 잠금 처리에서 **ONTAP**가 **Windows**와 어떻게 다른지 설명합니다

Windows와 달리 ONTAP는 파일이 열려 있는 동안 열려 있는 파일에 대한 경로의 각 구성 요소를 잠그지 않습니다. 이 동작은 SMB 공유 경로에도 영향을 줍니다.

ONTAP는 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.

ONTAP SMB 잠금에 대한 정보 표시

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. 에 대한 자세한 내용은 `vserver locks show` "ONTAP 명령 참조입니다"을 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
```

ONTAP SMB 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 locks break`명령은 advanced 권한 수준 이상에서만 사용할 수 있습니다. 에 대한 자세한 내용은 `vserver locks break` link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

단계

1. 잠금을 해제해야 하는 정보를 찾으려면 'vserver lock show' 명령을 사용합니다.

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

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

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

SMB 작업을 모니터링합니다

ONTAP SMB 세션 정보 표시

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 큽니다. 옵션 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다.

- 옵션 '-fields' 매개변수를 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
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'

SMB 세션 정보를 표시하려면…	다음 명령을 입력합니다…
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
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                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
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 **ONTAP SMB** 파일에 대한 정보 표시

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 큽니다. 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 **SMB** 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 **SMB** 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. 에 대한 자세한 내용은 `vserver cifs session file show` "ONTAP 명령 참조입니다"을 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::> vserver cifs session file show -vserver 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

세션 정보 표시

ONTAP SMB 서버에서 사용 가능한 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	`statistics catalog object show -object object_name`
사용할 수 있는 카운터	`statistics catalog counter show -object object_name`

   사용 가능한 개체 및 카운터를 비롯한 에 대한 자세한 `statistics catalog object show` 내용은 에서 "ONTAP 명령 참조입니다"알아보십시오.

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


[...]
```

관련 정보

- 통계를 표시합니다
- "통계 카탈로그 카운터 개체 표시"
- "통계 시작"

ONTAP SMB 통계 표시

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.

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

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'

   에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

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

관련 정보

- 서버에서 사용 가능한 통계, 개체 및 카운터를 확인합니다.
- SMB 서명 세션 통계 모니터링
- BranchCache 통계를 표시합니다
- 통계를 사용하여 자동 노드 조회 활동을 모니터링합니다

- "Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"
- "성능 모니터링 설정"