CLI를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다

ONTAP 9

NetApp
April 24, 2024

목차

CLI를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다

CLI 개요를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다

CLI를 사용하여 스토리지 가상 시스템(SVM)에서 NTFS 파일 보안, NTFS 감사 정책 및 스토리지 레벨 액세스 가드를 관리할 수 있습니다.

SMB 클라이언트 또는 CLI를 사용하여 NTFS 파일 보안 및 감사 정책을 관리할 수 있습니다. 그러나 CLI를 사용하여 파일 보안 및 감사 정책을 구성하면 원격 클라이언트를 사용하여 파일 보안을 관리할 필요가 없습니다. CLI를 사용하면 단일 명령을 사용하여 여러 파일과 폴더에 보안을 적용하는 데 걸리는 시간을 크게 줄일 수 있습니다.

ONTAP에서 SVM 볼륨에 적용한 또 다른 보안 계층인 스토리지 레벨 액세스 가드를 구성할 수 있습니다. Storage-Level Access Guard는 모든 NAS 프로토콜에서 Storage-Level Access Guard가 적용되는 스토리지 객체에 대한 액세스에 적용됩니다.

스토리지 레벨 액세스 가드는 ONTAP CLI에서만 구성 및 관리할 수 있습니다. SMB 클라이언트에서 스토리지 수준 액세스 가드 설정을 관리할 수 없습니다. 또한 NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다. 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 액세스 가드 보안을 취소할 수 없습니다. 따라서 Storage-Level Access Guard는 스토리지 관리자가 독립적으로 설정하고 관리하는 데이터 액세스를 위한 추가 보안 계층을 제공합니다.

> 스토리지 레벨 액세스 가드에 대해 NTFS 액세스 권한만 지원되지만, 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 정책에 대한 정보를 표시합니다

CLI를 사용하여 NTFS 파일 및 폴더에 파일 보안을 구성하고 적용합니다

CLI를 사용하여 NTFS 파일 및 폴더에 감사 정책을 구성하고 적용합니다

Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

CLI를 사용하여 파일 및 폴더 보안을 설정하는 사용 사례

원격 클라이언트의 개입 없이 로컬로 파일 및 폴더 보안을 적용 및 관리할 수 있으므로 많은 수의 파일 또는 폴더에 대해 대량 보안을 설정하는 데 걸리는 시간을 크게 줄일 수 있습니다.

CLI를 사용하여 다음과 같은 사용 사례에서 파일 및 폴더 보안을 설정할 수 있습니다.

- 홈 디렉토리의 파일 스토리지와 같은 대규모 엔터프라이즈 환경에 있는 파일의 스토리지
- 데이터 마이그레이션
- Windows 도메인 변경
- NTFS 파일 시스템 전반에 걸쳐 파일 보안 및 감사 정책 표준화

CLI를 사용하여 파일 및 폴더 보안을 설정할 때의 제한 사항

CLI를 사용하여 파일 및 폴더 보안을 설정할 때 특정 제한 사항을 알고 있어야 합니다.

- 'vserver security file-directory' 명령 제품군은 NFSv4 ACL 설정을 지원하지 않습니다.

  NTFS 보안 설명자는 NTFS 파일 및 폴더에만 적용할 수 있습니다.

보안 설명자를 사용하여 파일 및 폴더 보안을 적용하는 방법

보안 설명자는 사용자가 파일 및 폴더에 대해 수행할 수 있는 작업과 사용자가 파일 및 폴더에 액세스할 때 감사할 작업을 결정하는 액세스 제어 목록을 포함합니다.

- * 권한 *

권한은 개체의 소유자가 허용하거나 거부하고 개체(사용자, 그룹 또는 컴퓨터 개체)가 지정된 파일이나 폴더에서 수행할 수 있는 작업을 결정합니다.

- * 보안 설명자 *

  보안 설명자는 파일 또는 폴더와 관련된 권한을 정의하는 보안 정보가 포함된 데이터 구조입니다.

- * ACL(액세스 제어 목록) *

  액세스 제어 목록은 보안 설명자가 적용된 파일 또는 폴더에서 사용자, 그룹 또는 컴퓨터 개체가 수행할 수 있는 작업에 대한 정보를 포함하는 보안 설명자에 포함된 목록입니다. 보안 설명자는 다음 두 가지 유형의 ACL을 포함할 수 있습니다.

  - DACL(임의 액세스 제어 목록)
  - 시스템 액세스 제어 목록(SACL)

- * DACL(임의 액세스 제어 목록) *

  DACL에는 파일 또는 폴더에 대한 작업을 수행할 수 있는 액세스가 허용 또는 거부된 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. DACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- * 시스템 액세스 제어 목록(SACL) *

  SACL에는 성공 또는 실패 감사 이벤트가 기록되는 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. SACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- * ACE(액세스 제어 항목) *

  ACE는 DACL 또는 SACL의 개별 항목입니다.

  - DACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에 대해 허용 또는 거부된 액세스 권한을 지정합니다.
  - SACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에서 수행하는 지정된 작업을 감사할 때 기록할 성공 또는 실패 이벤트를 지정합니다.

- * 사용 권한 상속 *

  권한 상속에서는 보안 설명자에 정의된 권한이 부모 개체에서 개체로 전파되는 방법을 설명합니다. 상속 가능한 권한만 자식 개체에서 상속합니다. 상위 객체에 대한 권한을 설정할 때 폴더, 하위 폴더, 파일이 이 폴더에 적용, 하위 폴더, 파일 등을 통해 해당 항목을 상속할 수 있는지 여부를 결정할 수 있습니다.

관련 정보

"SMB 및 NFS 감사 및 보안 추적"

CLI를 사용하여 NTFS 파일 및 폴더에 감사 정책 구성 및 적용

SVM 재해 복구 대상에서 로컬 사용자 또는 그룹을 사용하는 파일 디렉토리 정책을 적용하기 위한 지침

파일 디렉토리 정책 구성에서 보안 설명자나 DACL 또는 SACL 항목의 로컬 사용자 또는 그룹을

사용하는 경우 ID 폐기 구성의 SVM(Storage Virtual Machine) 재해 복구 대상에 파일 디렉토리 정책을 적용하기 전에 염두에 두어야 할 몇 가지 지침이 있습니다.

소스 클러스터의 소스 SVM이 소스 SVM에서 데이터 및 구성을 소스 SVM에서 타겟 클러스터의 대상 SVM으로 복제하는 SVM을 위한 재해 복구 구성을 구성할 수 있습니다.

SVM 재해 복구의 두 가지 유형 중 하나를 설정할 수 있습니다.

- ID가 보존됩니다

  이 구성에서는 SVM과 CIFS 서버의 ID가 보존됩니다.

- ID가 삭제되었습니다

  이 구성에서는 SVM과 CIFS 서버의 ID가 유지되지 않습니다. 이 시나리오에서는 대상 SVM의 SVM 및 CIFS 서버의 이름이 소스 SVM의 SVM 및 CIFS 서버 이름과 다릅니다.

ID 폐기 구성에 대한 지침

로컬 사용자, 그룹 및 권한 구성이 포함된 SVM 소스의 경우 ID가 폐기된 구성에서 SVM 대상의 CIFS 서버 이름과 일치하도록 로컬 도메인(로컬 CIFS 서버 이름)의 이름을 변경해야 합니다. 예를 들어, 소스 SVM 이름이 ""VS1""이고 CIFS 서버 이름이 ""CIFS1""이고 대상 SVM 이름이 ""VS1_DST""이고 CIFS 서버 이름이 ""CIFS1_DST""인 경우 로컬 사용자 ""CIFS1\user1""의 로컬 도메인 이름이 ""FS1""""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

NTFS 보안 설명자를 만듭니다

NTFS 보안 설명자(파일 보안 정책)를 생성하는 것은 NTFS ACL(액세스 제어 목록)을 구성하여 SVM(스토리지 가상 머신) 내에 있는 파일 및 폴더에 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결할 수 있습니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

오브젝트	액세스 유형입니다	액세스 권한	사용 권한을 적용할 위치입니다
BUILTIN\Administrators입니다	허용	모든 권한	폴더, 하위 폴더, 파일
BUILTIN\사용자	허용	모든 권한	폴더, 하위 폴더, 파일
작성자 소유자	허용	모든 권한	폴더, 하위 폴더, 파일
NT AUTHORITY\SYSTEM	허용	모든 권한	폴더, 하위 폴더, 파일

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다
- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

NTFS DACL 액세스 제어 항목을 NTFS 보안 설명자에 추가합니다

NTFS 보안 설명자에 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)를 추가하는 것은 파일이나 폴더에 NTFS ACL을 구성하고 적용하는 두 번째 단계입니다. 각 항목은 액세스가

허용되거나 거부된 개체를 식별하고 ACE에 정의된 파일 또는 폴더에 대해 개체가 수행할 수 있거나 수행할 수 없는 작업을 정의합니다.

이 작업에 대해

보안 설명자의 DACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 DACL이 포함된 경우 명령은 새 ACE를 DACL에 추가합니다. 보안 설명자에 DACL이 포함되어 있지 않으면 명령에서 DACL을 생성하고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정에 대해 허용 또는 거부할 권한을 지정하여 DACL 항목을 선택적으로 사용자 지정할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)

> DACL 항목에 대한 권한을 지정하지 않으면 기본값은 "모든 권한"으로 설정됩니다.

선택적으로 상속 적용 방법을 지정하여 DACL 항목을 사용자 지정할 수 있습니다.

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

단계

1. 보안 설명자에 DACL 항목을 추가합니다. 'vserver security file -directory NTFS DACL add -vserver vserver_name -ntfs -sd sd sd_name -access -type {allow | deny} -account name_or_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
```

보안 정책을 생성합니다

SVM에 대한 파일 보안 정책을 생성하는 것은 파일이나 폴더에 ACL을 구성 및 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각 작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

단계

1. 'vserver security file-directory policy create-vserver vserver_name-policy-name policy_name' 보안 정책을 생성합니다

   'vserver security file-directory policy create-policy-name policy1-vserver vs1'

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
   Vserver           Policy Name
 ------------     --------------
     vs1               policy1
```

보안 정책에 작업을 추가합니다

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

  지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 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. 자세한 내용은 man 페이지를 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
```

보안 정책을 적용합니다

파일 또는 폴더에 NTFS ACL을 생성하고 적용하는 마지막 단계는 SVM에 파일 보안 정책을 적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.

> 감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

단계

1. 보안 정책('vserver security file-directory apply-vserver vserver_name -policy -name policy_name')을 적용합니다

   'vserver security file-directory apply-vserver vs1-policy-name policy1'

   정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

보안 정책 작업을 모니터링합니다

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용해야 합니다.

단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vserver_name'을 모니터링합니다

   'vserver security file-directory job show -vserver vs1'

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

적용된 파일 보안을 확인합니다

파일 보안 설정을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 머신)의 파일 또는 폴더에 원하는 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

보안 설정을 확인할 파일과 폴더의 경로와 데이터가 포함된 SVM의 이름을 제공해야 합니다. 옵션 '-Expand-mask' 매개변수를 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
```

CLI 개요를 사용하여 NTFS 파일 및 폴더에 감사 정책을 구성하고 적용합니다

ONTAP CLI를 사용할 때 NTFS 파일 및 폴더에 감사 정책을 적용하려면 몇 가지 단계를 수행해야 합니다. 먼저 NTFS 보안 설명자를 만들고 보안 설명자에 SACL을 추가합니다. 그런 다음 보안 정책을 만들고 정책 작업을 추가합니다. 그런 다음 SVM(스토리지 가상 시스템)에 보안 정책을 적용합니다.

이 작업에 대해

보안 정책을 적용한 후 보안 정책 작업을 모니터링하고 적용된 감사 정책의 설정을 확인할 수 있습니다.

> 감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

관련 정보

Storage-Level Access Guard를 사용하여 파일 액세스 보호

CLI를 사용하여 파일 및 폴더 보안을 설정할 때의 제한 사항

보안 설명자를 사용하여 파일 및 폴더 보안을 적용하는 방법

"SMB 및 NFS 감사 및 보안 추적"

CLI를 사용하여 NTFS 파일 및 폴더에 파일 보안을 구성하고 적용합니다

NTFS 보안 설명자를 만듭니다

NTFS 보안 설명자 감사 정책을 생성하는 것은 SVM에 상주하는 파일 및 폴더에 NTFS ACL(액세스 제어 목록)을 구성 및 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결합니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

오브젝트	액세스 유형입니다	액세스 권한	사용 권한을 적용할 위치입니다
BUILTIN\Administrators입니다	허용	모든 권한	폴더, 하위 폴더, 파일
BUILTIN\사용자	허용	모든 권한	폴더, 하위 폴더, 파일
작성자 소유자	허용	모든 권한	폴더, 하위 폴더, 파일
NT AUTHORITY\SYSTEM	허용	모든 권한	폴더, 하위 폴더, 파일

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다
- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 man 페이지를 참조하십시오.

단계

1. 고급 매개 변수를 사용하려면 권한 수준을 고급:'Set-Privilege Advanced'로 설정합니다
2. 보안 설명자:'vserver security file-directory NTFS create-vserver 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

NTFS SACL 액세스 제어 항목을 NTFS 보안 설명자에 추가합니다

SACL(시스템 액세스 제어 목록) ACE(액세스 제어 항목)를 NTFS 보안 설명자에 추가하는 것은 SVM의 파일 또는 폴더에 대한 NTFS 감사 정책을 생성하는 두 번째 단계입니다. 각 항목은 감사하려는 사용자 또는 그룹을 식별합니다. SACL 항목은 성공한 액세스 시도 또는 실패한

액세스 시도를 감사할지 여부를 정의합니다.

이 작업에 대해

보안 설명자의 SACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 SACL이 포함된 경우 이 명령은 새 ACE를 SACL에 추가합니다. 보안 설명자에 SACL이 포함되어 있지 않으면 명령에서 SACL을 만들고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정의 성공 또는 실패 이벤트에 대해 감사할 권한을 지정하여 SACL 항목을 구성할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)

> SACL 항목에 대한 권한을 지정하지 않으면 기본 설정은 "모든 권한"입니다.

"apply to" 매개 변수를 사용하여 상속을 적용하는 방법을 지정하여 SACL 항목을 선택적으로 사용자 지정할 수 있습니다. 이 매개 변수를 지정하지 않으면 기본적으로 이 SACL 항목을 이 폴더, 하위 폴더 및 파일에 적용합니다.

단계

1. 보안 설명자에 SACL 항목을 추가합니다. 'vserver security file-directory NTFS SACL add -vserver 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
```

보안 정책을 생성합니다

SVM(스토리지 가상 머신)에 대한 감사 정책을 생성하는 것은 ACL을 구성하여 파일 또는 폴더에 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각

작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(스토리지 가상 머신)(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

단계

1. 'vserver security file-directory policy create-vserver vserver_name-policy-name policy_name' 보안 정책을 생성합니다

   'vserver security file-directory policy create-policy-name policy1-vserver vs1'

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

보안 정책에 작업을 추가합니다

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

  지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 디렉토리 작업을 통해 적용된 ACL은 SMB 클라이언트 또는 ONTAP CLI를 통해 관리할 수 있습니다.

- 스토리지 레벨 액세스 가드 작업

  지정된 볼륨에 Storage-Level Access Guard 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 스토리지 레벨 액세스 가드 작업을 통해 적용된 ACL은 ONTAP CLI를 통해서만 관리할 수 있습니다.

작업에는 파일(또는 폴더) 또는 파일 집합(또는 폴더)의 보안 구성에 대한 정의가 포함됩니다. 정책의 모든 작업은 경로로 고유하게 식별됩니다. 단일 정책 내에서 경로당 하나의 작업만 있을 수 있습니다. 정책에 중복된 작업 항목이 있을 수 없습니다.

정책에 작업 추가 지침:

- 정책당 최대 10,000개의 작업 항목이 있을 수 있습니다.
- 정책에는 하나 이상의 작업이 포함될 수 있습니다.

  정책에 둘 이상의 작업이 포함될 수 있지만 파일 디렉터리 및 저장소 수준 액세스 가드 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 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. 자세한 내용은 man 페이지를 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
```

보안 정책을 적용합니다

파일 또는 폴더에 NTFS ACL을 생성하고 적용하는 마지막 단계는 SVM에 감사 정책을 적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.

> 감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

단계

1. 'vserver security file-directory apply-vserver vserver_name-policy-name policy_name' 보안 정책을 적용합니다

   'vserver security file-directory apply-vserver vs1-policy-name policy1'

   정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

보안 정책 작업을 모니터링합니다

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용해야 합니다.

단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vserver_name'을 모니터링합니다

   'vserver security file-directory job show -vserver vs1'

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

적용된 감사 정책을 확인합니다

감사 정책을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 시스템)의 파일 또는 폴더에 원하는 감사 보안 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

'vserver security file-directory show' 명령을 사용하여 감사 정책 정보를 표시합니다. 표시할 파일 또는 폴더 감사 정책 정보를 가진 데이터의 경로와 데이터가 들어 있는 SVM의 이름을 제공해야 합니다.

단계

1. 감사 정책 설정 표시: 'vserver security file-directory show -vserver_vserver_name_-path_path_'

예

다음 명령을 실행하면 SVM VS1 경로의 ""/Corp" 경로에 적용된 감사 정책 정보가 표시됩니다. 경로에 성공 및 성공/실패 SACL 항목이 모두 적용됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

보안 정책 작업을 관리할 때의 고려 사항

특정 상황에서 보안 정책 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을

수정할 수 없습니다. 정책을 수정할 수 있는 조건이나 수정할 수 없는 조건을 이해해야 정책을 수정할 수 있습니다. 정책 수정에는 정책에 할당된 작업을 추가, 제거 또는 수정하고 정책을 삭제 또는 수정하는 작업이 포함됩니다.

해당 정책에 대한 작업이 있고 해당 작업이 다음 상태인 경우 해당 정책에 할당된 보안 정책 또는 작업을 수정할 수 없습니다.

- 작업이 실행 중이거나 진행 중입니다.
- 작업이 일시 중지되었습니다.
- 작업이 재개되고 실행 중 상태입니다.
- 작업이 다른 노드로 장애 조치를 기다리는 경우

다음 상황에서 보안 정책에 대한 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을 성공적으로 수정할 수 있습니다.

- 정책 작업이 중지되었습니다.
- 정책 작업이 성공적으로 완료되었습니다.

NTFS 보안 설명자를 관리하는 명령입니다

보안 설명자를 관리하기 위한 특정 ONTAP 명령이 있습니다. 보안 설명자에 대한 정보를 생성, 수정, 삭제 및 표시할 수 있습니다.

원하는 작업	이 명령 사용...
NTFS 보안 설명자를 만듭니다	'vserver security file-directory NTFS create'
기존 NTFS 보안 설명자를 수정합니다	'vserver security file-directory NTFS modify'를 참조하십시오
기존 NTFS 보안 설명자에 대한 정보를 표시합니다	'vserver security file-directory NTFS show'
NTFS 보안 설명자를 삭제합니다	'vserver security file-directory NTFS delete

자세한 내용은 가상 서버 보안 파일 디렉토리 NTFS 명령에 대한 man 페이지를 참조하십시오.

NTFS DACL 액세스 제어 항목을 관리하는 명령입니다

DACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS DACL에 추가할 수 있습니다. DACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS DACL을 관리할 수도 있습니다.

원하는 작업	이 명령 사용...
ACE를 만들어 NTFS DACL에 추가합니다	'vserver security file-directory NTFS DACL add'
NTFS DACL에서 기존 ACE를 수정합니다	'vserver security file-directory NTFS DACL modify'를 선택합니다
NTFS DACL의 기존 ACE에 대한 정보를 표시합니다	'vserver security file-directory NTFS DACL show'
NTFS DACL에서 기존 ACE를 제거합니다	'vserver security file-directory NTFS DACL remove'

자세한 내용은 'vserver security file-directory NTFS DACL' 명령에 대한 man 페이지를 참조하십시오.

NTFS SACL 액세스 제어 항목을 관리하는 명령입니다

SACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS SACL에 추가할 수 있습니다. SACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS SACL을 관리할 수도 있습니다.

원하는 작업	이 명령 사용...
ACE를 만들어 NTFS SACL에 추가합니다	'vserver security file-directory NTFS SACL add'
NTFS SACL에서 기존 ACE를 수정합니다	'vserver security file-directory NTFS SACL modify'를 참조하십시오
NTFS SACL의 기존 ACE에 대한 정보를 표시합니다	'vserver security file-directory NTFS SACL show'
NTFS SACL에서 기존 ACE를 제거합니다	'vserver security file-directory NTFS SACL remove'

자세한 내용은 'vserver security file-directory NTFS SACL' 명령에 대한 man 페이지를 참조하십시오.

보안 정책 관리를 위한 명령입니다

보안 정책을 관리하기 위한 특정 ONTAP 명령이 있습니다. 정책에 대한 정보를 표시하고 정책을 삭제할 수 있습니다. 보안 정책을 수정할 수 없습니다.

원하는 작업	이 명령 사용...
보안 정책을 생성합니다	'vserver security file-directory policy create'를 참조하십시오
보안 정책에 대한 정보를 표시합니다	'vserver security file-directory policy show'를 선택합니다

원하는 작업	이 명령 사용...
보안 정책을 삭제합니다	'vserver security file-directory policy delete

자세한 내용은 'vserver security file-directory policy' 명령에 대한 man 페이지를 참조하십시오.

보안 정책 작업을 관리하기 위한 명령입니다

보안 정책 작업에 대한 정보를 추가, 수정, 제거 및 표시하는 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
보안 정책 작업을 추가합니다	'vserver security file-directory policy task add'
보안 정책 작업을 수정합니다	'vserver security file-directory policy task modify'를 선택합니다
보안 정책 작업에 대한 정보를 표시합니다	'vserver security file-directory policy task show'를 선택합니다
보안 정책 작업을 제거합니다	'vserver security file-directory policy task remove'

자세한 내용은 'vserver security file-directory policy task' 명령에 대한 man 페이지를 참조하십시오.

보안 정책 작업 관리를 위한 명령입니다

보안 정책 작업에 대한 정보를 일시 중지, 다시 시작, 중지 및 표시하는 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
보안 정책 작업을 일시 중지합니다	'vserver security file-directory job pause -vserver vserver_name -id integer'
보안 정책 작업을 다시 시작합니다	'vserver security file-directory job resume - vserver vserver_name -id integer'
보안 정책 작업에 대한 정보를 표시합니다	'vserver security file-directory job show -vserver_name' 이 명령을 사용하여 작업의 작업 ID를 확인할 수 있습니다.
보안 정책 작업을 중지합니다	'vserver security file-directory job stop -vserver vserver_name -id integer'

자세한 내용은 'vserver security file-directory job' 명령에 대한 man 페이지를 참조하십시오.