



CLI를 사용하여 **NTFS** 파일 및 폴더에 파일 보안을 구성하고 적용합니다

ONTAP 9

NetApp
April 24, 2024

목차

CLI를 사용하여 NTFS 파일 및 폴더에 파일 보안을 구성하고 적용합니다	1
NTFS 보안 설명자를 만듭니다	1
NTFS DACL 액세스 제어 항목을 NTFS 보안 설명자에 추가합니다	1
보안 정책을 생성합니다	2
보안 정책에 작업을 추가합니다	3
보안 정책을 적용합니다	5
보안 정책 작업을 모니터링합니다	5
적용된 파일 보안을 확인합니다	6

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 vs1 -ntfs -sd sd1 -access-type {allow | deny} -account domain\joe'

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

2. DACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS DACL show -vserver vs1 -ntfs -sd sd1 -access-type {allow|deny} -account domain\joe'

```
'vserver security file-directory NTFS DACL show -vserver vs1-ntfs-sd SD1-access-type deny-account
domain\joe'
```

```
Vserver: vs1
Security Descriptor Name: sd1
    Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
    Access Rights: full-control
Advanced Access Rights: -
    Apply To: this-folder
    Access Rights: full-control
```

보안 정책을 생성합니다

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

이 작업에 대해

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

단계

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

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

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

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

보안 정책에 작업을 추가합니다

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

이 작업에 대해

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

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

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

- 스토리지 레벨 액세스 가드 작업

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

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

정책에 작업 추가 지침:

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

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

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

추가 액세스 권한은 제공하지 않습니다.

보안 정책에 작업을 추가할 때 다음 네 가지 필수 매개 변수를 지정해야 합니다.

- SVM 이름
- 정책 이름입니다
- 경로
- 경로와 연결할 보안 설명자입니다

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

- 보안 유형입니다
- 전파 모드
- 인덱스 위치
- 액세스 제어 유형입니다

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

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉터리 정책 작업 추가 - vserverserver_name -policy -name policy_name -path path -NTFS-SD_nameoptional_parameters'

파일 디렉터리는 '-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 server_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 vs1-policy-name policy1')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 vs1'을 모니터링합니다

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

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

적용된 파일 보안을 확인합니다

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

이 작업에 대해

보안 설정을 확인할 파일과 폴더의 경로와 데이터가 포함된 SVM의 이름을 제공해야 합니다. 옵션 '-Expand-mask' 매개 변수를 사용하여 보안 설정에 대한 자세한 정보를 표시할 수 있습니다.

단계

1. 파일 및 폴더 보안 설정 표시: 'vserver security file-directory show -vserver vs1-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	

Read Attributes1.... =
Delete Child1... =
Execute1... =
Write EA1... =
Read EA1... =
Append1... =
Write1... =
Read1... =
ALLOW-Everyone-0x10000000-OI CI IO	
Generic Read	0..... =
Generic Write	.0..... =
Generic Execute	..0..... =
Generic All	...1..... =
System Security0..... =
Synchronize0..... =
Write Owner0..... =
Write DAC0..... =
Read Control0..... =
Delete0..... =
Write Attributes0..... =
Read Attributes0..... =
Delete Child0..... =
Execute0..... =

Write EA0..... =
Read EA0... =
Append0.. =
Write0. =
Read0 =

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.