



## 우회 통과 검사를 구성합니다 ONTAP 9

NetApp  
April 24, 2024

# 목차

우회 통과 검사를 구성합니다.....	1
우회 횡단 검사 개요 구성 .....	1
사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다.....	2
디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다.....	3

# 우회 통과 검사를 구성합니다

## 우회 횡단 검사 개요 구성

통과 확인 무시 사용자 권한(\_privilege\_라고도 함)은 사용자가 이동 중인 디렉터리에 대한 권한이 없더라도 경로 내의 모든 디렉터리를 파일로 이동할 수 있는지 여부를 결정합니다. 통과 확인을 허용 또는 허용하지 않을 경우 어떤 일이 발생하는지, 그리고 SVM(스토리지 가상 시스템)에서 사용자에게 대한 통과 확인을 건너뛰도록 구성하는 방법을 이해해야 합니다.

### 우회 통과 확인을 허용 또는 허용하지 않을 때 발생하는 현상

- 허용되는 경우 사용자가 파일에 액세스하려고 할 때 ONTAP은 파일에 대한 액세스 허용 또는 거부 여부를 결정할 때 중간 디렉터리에 대한 통과 권한을 확인하지 않습니다.
- 허용되지 않는 경우 ONTAP은 파일 경로에 있는 모든 디렉터리에 대해 트래버스(실행) 권한을 확인합니다.

중간 디렉터리에 ""X""(통과 권한)이 없으면 ONTAP은 해당 파일에 대한 액세스를 거부합니다.

## 우회 통과 검사를 구성합니다

ONTAP CLI를 사용하거나 이 사용자 권한으로 Active Directory 그룹 정책을 구성하여 통과 통과 확인 바이패스를 구성할 수 있습니다.

'eChangeNotifyPrivilege' 권한은 사용자가 횡단 확인을 우회할 수 있는지 여부를 제어합니다.

- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에 추가하면 통과 확인을 건너뛸 수 있습니다.
- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에서 제거하면 통과 확인을 건너뛸 수 없습니다.

기본적으로 SVM의 다음 BUILTIN 그룹에는 횡단 확인을 건너뛸 수 있는 권한이 있습니다.

- 'BUILTIN\Administrators'
- 'BUILTIN\Power Users'
- 'BUILTIN\Backup Operators'
- 'BUILTIN\Users'
- '모든 사람'

이러한 그룹 중 하나의 구성원이 통과 확인을 건너뛰도록 허용하지 않으려면 그룹에서 이 권한을 제거해야 합니다.

CLI를 사용하여 SVM에서 로컬 SMB 사용자 및 그룹에 대한 통과 검사를 구성할 때 다음 사항을 염두에 두어야 합니다.

- 사용자 지정 로컬 또는 도메인 그룹의 구성원이 통과 확인을 건너뛰도록 하려면 해당 그룹에 'eChangeNotifyPrivilege' 권한을 추가해야 합니다.
- 개별 로컬 또는 도메인 사용자가 횡단 검사를 무시하도록 허용하고 해당 권한이 있는 그룹의 구성원이 아닌 경우 해당 사용자 계정에 'eChangeNotifyPrivilege' 권한을 추가할 수 있습니다.
- 언제든지 'ChangeNotifyPrivilege' 권한을 제거하여 로컬 또는 도메인 사용자 또는 그룹에 대한 통과 확인을 사용하지 않도록 설정할 수 있습니다.



지정된 로컬 또는 도메인 사용자 또는 그룹에 대한 우회 트래버스 검사를 비활성화하려면 "Everyone" 그룹에서 'ChangeNotifyPrivilege' 권한도 제거해야 합니다.

#### 관련 정보

사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다

디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다

볼륨에서 SMB 파일 이름 변환에 대한 문자 매핑을 구성합니다

SMB 공유 액세스 제어 목록을 생성합니다

Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

지원되는 권한 목록입니다

로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다

## 사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다

사용자가 이동 중인 디렉토리에 대한 사용 권한이 없더라도 경로 내의 모든 디렉토리를 통과할 수 있도록 하려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하면 됩니다. 기본적으로 사용자는 디렉터리 통과 확인을 건너뛸 수 있습니다.

#### 시작하기 전에

- SVM에 SMB 서버가 있어야 합니다.
- 로컬 사용자 및 그룹 SMB 서버 옵션을 활성화해야 합니다.
- 'seChangeNotifyPrivilege' 권한을 추가할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

#### 이 작업에 대해

도메인 사용자 또는 그룹에 권한을 추가할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

#### 단계

1. 로컬 또는 도메인 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하여 통과 확인을 사용하지 않도록 설정합니다. 'vserver cifs users-and-groups privilege add-privilege\_vserver\_name\_-user-or-group-name\_name\_-Privileges SeChangeNotifyPrivilege'

'-user-or-group-name' 매개 변수의 값은 로컬 사용자 또는 그룹 또는 도메인 사용자 또는 그룹입니다.

2. 지정된 사용자 또는 그룹이 통과 확인 생략 기능을 사용하도록 설정했는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_'

#### 예

다음 명령을 사용하면 "Example\eng" 그룹에 속한 사용자가 'seChangeNotifyPrivilege' 권한을 그룹에 추가하여 디렉터리 통과 확인을 건너뛸 수 있습니다.

```
cluster1::> vsserver cifs users-and-groups privilege add-privilege -vsserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vsserver cifs users-and-groups privilege show -vsserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng             SeChangeNotifyPrivilege
```

#### 관련 정보

사용자 또는 그룹이 디렉터리 트래버스 검사를 건너뛰는 것을 허용하지 않습니다

## 디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다

사용자가 이동 중인 디렉토리에 대한 권한이 없기 때문에 경로 내의 모든 디렉토리를 이동하지 않으려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에서 'seChangeNotifyPrivilege' 권한을 제거할 수 있습니다.

#### 시작하기 전에

권한을 제거할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

#### 이 작업에 대해

도메인 사용자 또는 그룹에서 권한을 제거할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

#### 단계

1. 통과 확인 무시 허용 안 함: 'vsserver cifs users-and-groups privilege remove-privilege-vsserver\_vsserver\_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. 'vsserver cifs users-and-groups privilege show-vsserver\_name\_-user-or-group-name\_name\_'

#### 예

다음 명령을 실행하면 디렉터리 트래버스 검사를 거치지 않고 "example\eng" 그룹에 속한 사용자가 사용할 수 없습니다.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	EXAMPLE\eng	SeChangeNotifyPrivilege

```
cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	EXAMPLE\eng	-

#### 관련 정보

[사용자 또는 그룹이 디렉토리 통과 확인을 생략하도록 허용합니다](#)

## 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.