



Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

ONTAP 9

NetApp
April 24, 2024

Inhalt

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI	1
Erstellen Sie einen NTFS-Sicherheitsdeskriptor	1
Fügen Sie dem NTFS-Sicherheitsdeskriptor NTFS-DACL-Zugriffssteuerungseinträge hinzu	2
Erstellen von Sicherheitsrichtlinien	3
Fügen Sie der Sicherheitsrichtlinie eine Aufgabe hinzu	3
Wenden Sie Sicherheitsrichtlinien an	5
Überwachen Sie den Job der Sicherheitsrichtlinie	6
Überprüfen Sie die angewendete Dateisicherheit	6

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Erstellen Sie einen NTFS-Sicherheitsdeskriptor

Das Erstellen eines NTFS-Sicherheitsdeskriptors (Dateisicherheitsrichtlinie) ist der erste Schritt bei der Konfiguration und Anwendung von NTFS-Zugriffssteuerungslisten (NTFS Access Control Lists, ACLs) auf Dateien und Ordner innerhalb der Storage Virtual Machines (SVMs). Sie können den Sicherheitsdeskriptor in einer Richtlinienaufgabe dem Datei- oder Ordnerpfad zuordnen.

Über diese Aufgabe

NTFS-Sicherheitsdeskriptoren können für Dateien und Ordner erstellt werden, die sich in NTFS-Volumes im Sicherheitsstil befinden, oder für Dateien und Ordner, die sich auf gemischten Volumes im Sicherheitsstil befinden.

Wenn ein Sicherheitsdeskriptor erstellt wird, werden standardmäßig vier DACL-Einträge (Discretionary Access Control List) zur Sicherheitsbeschreibung hinzugefügt. Die vier Standard-Aces sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Anwenden der Berechtigungen
BUILTIN\Administratoren	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
BUILTIN\Benutzer	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
CREATOR-BESITZER	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Besitzer des Sicherheitsdeskriptors
- Primäre Gruppe des Eigentümers
- RAW-Kontrollfahnen

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Fügen Sie dem NTFS-Sicherheitsdeskriptor NTFS-DACL-Zugriffssteuerungseinträge hinzu

Das Hinzufügen von DACL (Ermessensliste für die Zugriffssteuerung) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Konfiguration und Anwendung von NTFS-ACLs auf eine Datei oder einen Ordner. Jeder Eintrag identifiziert, welches Objekt erlaubt oder verweigert wird, und definiert, was das Objekt für die im ACE definierten Dateien oder Ordner tun kann oder nicht.

Über diese Aufgabe

Sie können eine oder mehrere Asse zur DACL des Sicherheitsdeskriptors hinzufügen.

Wenn der Sicherheitsdeskriptor eine DACL enthält, die Asse enthält, fügt der Befehl den neuen ACE zum DACL hinzu. Wenn der Sicherheitsdeskriptor keine DACL enthält, erstellt der Befehl die DACL und fügt den neuen ACE hinzu.

Sie können optional DACL-Einträge anpassen, indem Sie angeben, welche Rechte Sie für das in angegebene Konto zulassen oder verweigern möchten `-account` Parameter. Es gibt drei Methoden, die sich gegenseitig ausschließen, um Rechte anzugeben:

- Rechte
- Erweiterte Rechte
- RAW-Rechte (Advanced-Privilege)



Wenn Sie keine Rechte für den DACL-Eintrag angeben, werden standardmäßig die Rechte auf festgelegt `Full Control`.

Sie können optional DACL-Einträge anpassen, indem Sie festlegen, wie Vererbung angewendet wird.

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Hinzufügen eines DACL-Eintrags zu einem Sicherheitsdeskriptor: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID optional_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. Überprüfen Sie, ob der DACL-Eintrag korrekt ist: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-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
```

Erstellen von Sicherheitsrichtlinien

Das Erstellen einer Dateisicherheitsrichtlinie für SVMs ist der dritte Schritt beim Konfigurieren und Anwenden von ACLs auf eine Datei oder einen Ordner. Eine Richtlinie fungiert als Container für verschiedene Aufgaben, wobei jede Aufgabe ein einzelner Eintrag ist, der auf Dateien oder Ordner angewendet werden kann. Sie können Aufgaben später der Sicherheitsrichtlinie hinzufügen.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollten Sie die Sicherheitsrichtlinie jeder SVM zuweisen (die NTFS Security-Volumes oder Volumes im gemischten Sicherheitsstil enthält).

Schritte

1. Sicherheitsrichtlinie erstellen: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. Überprüfen Sie die Sicherheitsrichtlinie: `vserver security file-directory policy show`

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

Fügen Sie der Sicherheitsrichtlinie eine Aufgabe hinzu

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt bei der Konfiguration und Anwendung von ACLs auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe verknüpfen Sie die Aufgabe mit einer Sicherheitsrichtlinie. Sie können einer Sicherheitsrichtlinie einen oder mehrere Aufgabeneinträge hinzufügen.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf einen einzelnen Vorgang, der von einer Sicherheitsrichtlinie auf Dateien oder Ordner mit NTFS oder gemischter Sicherheit (oder auf ein Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. ACLs, die über Datei- und Verzeichnisaufgaben angewendet werden, können mit SMB-Clients oder der ONTAP CLI gemanagt werden.

- Storage-Level Access Guard-Aufgaben

Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf Storage-Ebene für den Access Guard auf ein angegebenes Volume anwenden. ACLs, die über Aufgaben der Storage-Ebene Access Guard angewendet werden, können nur über die ONTAP-CLI gemanagt werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder eines Dateiansatz (oder Ordners). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Es kann nur eine Aufgabe pro Pfad innerhalb einer einzigen Richtlinie geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10,000 Aufgabeneinträge eingegeben werden.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

Obwohl eine Richtlinie mehr als eine Aufgabe enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Dateiverzeichnisaufgaben als auch Zugriffsschutz auf Speicherebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

Es wird niemals zusätzliche Zugriffsrechte geben.

Beim Hinzufügen von Aufgaben zu Sicherheitsrichtlinien müssen Sie die folgenden vier erforderlichen Parameter angeben:

- SVM-Name
- Name der Richtlinie
- Pfad
- Sicherheitsdeskriptor, der mit dem Pfad verknüpft wird

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus

- Indexposition
- Art der Zugriffskontrolle

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor hinzu:

```
vserver security file-directory policy task add -vserver vserver_name -policy
-name policy_name -path path -ntfs-sd SD_nameoptional_parameters
```

`file-directory` ist der Standardwert für `-access-control` Parameter. Die Angabe des Zugriffstypstyps bei der Konfiguration von Aufgaben für den Datei- und Verzeichniszugriff ist optional.

```
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
```

2. Überprüfen Sie die Aufgabenkonfiguration der Richtlinie: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

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

Wenden Sie Sicherheitsrichtlinien an

Der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner ist die Anwendung einer Dateisicherheitsrichtlinie auf SVMs.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie festgelegten Sicherheitseinstellungen auf NTFS-Dateien und Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder unterschiedlicher Sicherheitsstil).



Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Wenn eine Sicherheitsrichtlinie und die zugehörigen DACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Schritt

1. Anwenden einer Sicherheitsrichtlinie: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

Der Policy Apply Job ist geplant und die Job-ID wird zurückgegeben.

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

Überwachen Sie den Job der Sicherheitsrichtlinie

Wenn Sie die Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) anwenden, können Sie den Fortschritt der Aufgabe durch Monitoring des Jobs mit den Sicherheitsrichtlinien überwachen. Dies ist hilfreich, wenn Sie feststellen möchten, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn Sie einen langen Job haben, bei dem Sie Massensicherheit auf eine große Anzahl von Dateien und Ordnern anwenden.

Über diese Aufgabe

Um detaillierte Informationen über einen Job für Sicherheitsrichtlinien anzuzeigen, sollten Sie den verwenden `-instance` Parameter.

Schritt

1. Überwachen Sie den Job der Sicherheitsrichtlinie: `vserver security file-directory job show -vserver vserver_name`

```
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				

Überprüfen Sie die angewendete Dateisicherheit

Sie können die Dateisicherheitseinstellungen überprüfen, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die Sie die Sicherheitsrichtlinie angewendet haben, die gewünschten Einstellungen aufweisen.

Über diese Aufgabe

Sie müssen den Namen der SVM angeben, die die Daten sowie den Pfad zu der Datei und den Ordnern enthält, auf denen Sie die Sicherheitseinstellungen überprüfen möchten. Sie können das optionale verwenden

-expand-mask Parameter zum Anzeigen detaillierter Informationen zu den Sicherheitseinstellungen.

Schritt

1. Sicherheitseinstellungen für Datei und Ordner anzeigen: `vserver security file-directory show -vserver vserver_name -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										

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 =	

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.