Sicherheitsstile konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/security-styles-their-effects-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Sicherheitsstile konfigurieren . . . 1
Informationen zu ONTAP SMB-Sicherheitsstilen und deren Auswirkungen . . . 1
Informationen zur Vererbung des Sicherheitsstils bei ONTAP SMB . . . 2
SMB-Sicherheitsstile auf ONTAP SVM Root-Volumes konfigurieren . . . 3
SMB-Sicherheitsstile auf ONTAP FlexVol Volumes konfigurieren . . . 3
SMB-Sicherheitsstile auf ONTAP Qtrees konfigurieren . . . 4

Sicherheitsstile konfigurieren

Informationen zu ONTAP SMB-Sicherheitsstilen und deren Auswirkungen

Es gibt vier verschiedene Sicherheitsstile: UNIX, NTFS, gemischt und einheitlich. Jeder Sicherheitsstil wirkt sich unterschiedlich darauf aus, wie Berechtigungen für Daten gehandhabt werden. Das Verständnis der unterschiedlichen Auswirkungen ist erforderlich, um den passenden Sicherheitsstil für die jeweiligen Zwecke auszuwählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht festlegen, welche Clienttypen auf Daten zugreifen dürfen oder nicht. Sicherheitsstile bestimmen lediglich die Art der Berechtigungen, die ONTAP zur Steuerung des Datenzugriffs verwendet, und welcher Clienttyp diese Berechtigungen ändern darf.

Wenn beispielsweise ein Volume den UNIX-Sicherheitsstil verwendet, können SMB-Clients weiterhin auf Daten zugreifen (sofern sie ordnungsgemäß authentifizieren und autorisieren), da ONTAP multiprotokollfähig ist. ONTAP verwendet jedoch UNIX-Berechtigungen, die nur UNIX-Clients mit nativen Tools ändern können.

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Resultierender effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Unix	NFS	• NFSv3 Modusbits • NFSv4.x-ACLs	Unix	NFS und SMB
NTFS	SMB	NTFS-ACLs	NTFS	NFS und SMB
Gemischt	NFS oder SMB	• NFSv3 Modusbits • NFSv4.x-ACLs • NTFS-ACLs	• UNIX (für NFSv3-Modusbits und NFSv4.x-ACLs) • NTFS (für NTFS-ACLs)	NFS und SMB
Unified (Nur für unbegrenzte Volumes, in ONTAP 9.4 und früheren Versionen.)	NFS oder SMB	• NFSv3 Modusbits • NFSv4.1-ACLs • NTFS-ACLs	• UNIX (für NFSv3-Modusbits und NFSv4.1-ACLs) • NTFS (für NTFS-ACLs)	NFS und SMB

FlexVol Volumes unterstützen UNIX, NTFS und gemischte Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder einheitlich ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil individuell festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modusbits. Wenn der letzte Client ein NFSv4-Client war, sind die Berechtigungen NFSv4-ACLs. Wenn der letzte Client ein SMB-Client war, sind die Berechtigungen Windows NTFS-ACLs.

Der einheitliche Sicherheitsstil ist nur mit unbegrenzten Volumes verfügbar, die in ONTAP 9.5 und späteren Versionen nicht mehr unterstützt werden. Weitere Informationen finden sich unter FlexGroup Volumenmanagement-Übersicht.

Der `show-effective-permissions` Parameter mit dem `vserver security file-directory` Befehl ermöglicht die Anzeige der effektiven Berechtigungen, die einem Windows- oder UNIX-Benutzer für den angegebenen Datei- oder Ordnerpfad gewährt wurden. Zusätzlich ermöglicht der optionale Parameter `-share-name` die Anzeige der effektiven Freigabeberechtigung. Weitere Informationen zu `vserver security file-directory show-effective-permissions` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP legt zunächst einige Standard-Dateiberechtigungen fest. Standardmäßig ist der effektive Sicherheitsstil für alle Daten in UNIX-, gemischten und einheitlichen Security-Style-Volumes UNIX, und der effektive Berechtigungstyp ist UNIX-Modusbits (0755, sofern nicht anders angegeben), bis ein Client die Berechtigungen gemäß dem Standard-Sicherheitsstil konfiguriert. Standardmäßig ist der effektive Sicherheitsstil für alle Daten in NTFS-Security-Style-Volumes NTFS, und es besteht eine ACL, die allen Benutzern vollständige Kontrolle erlaubt.

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Sicherheitsstile können auf FlexVol-Volumes (sowohl Root- als auch Datenvolumes) und qtrees festgelegt werden. Sicherheitsstile können manuell bei der Erstellung festgelegt, automatisch übernommen oder zu einem späteren Zeitpunkt geändert werden. == Entscheiden Sie, welche SMB-Sicherheitsstile auf ONTAP SVMs verwendet werden sollen

Zur Unterstützung bei der Entscheidung, welchen Sicherheitsstil Sie für ein Volume verwenden, sind zwei Faktoren zu berücksichtigen. Der wichtigste Faktor ist die Art des Administrators, der das Dateisystem verwaltet. Der zweite Faktor ist die Art des Benutzers oder Dienstes, der auf die Daten auf dem Volume zugreift.

Bei der Konfiguration des Sicherheitsstils eines Volumes sollten die Anforderungen Ihrer Umgebung berücksichtigt werden, um den optimalen Sicherheitsstil auszuwählen und Probleme bei der Berechtigungsverwaltung zu vermeiden. Die folgenden Überlegungen können bei der Entscheidung helfen:

Sicherheitsstil	Wählen Sie aus, ob…
UNIX	• Das Dateisystem wird von einem UNIX-Administrator verwaltet. • Die Mehrheit der Nutzer sind NFS-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen UNIX-Benutzer als Dienstkonto.
NTFS	• Das Dateisystem wird von einem Windows-Administrator verwaltet. • Die Mehrheit der Nutzer sind SMB-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen Windows-Benutzer als Dienstkonto.
Gemischt	Das Dateisystem wird sowohl von UNIX- als auch von Windows-Administratoren verwaltet, und die Benutzer bestehen sowohl aus NFS- als auch aus SMB-Clients.

Informationen zur Vererbung des Sicherheitsstils bei ONTAP SMB

Wenn Sie beim Erstellen eines neuen FlexVol volume oder eines qtree keinen Sicherheitsstil angeben, wird der Sicherheitsstil auf unterschiedliche Weise übernommen.

Sicherheitsstile werden folgendermaßen vererbt:

- Ein FlexVol volume übernimmt den Sicherheitsstil des Root-Volumes der SVM, in der es enthalten ist.
- Ein Qtree erbt den Sicherheitsstil des ihn enthaltenden FlexVol volume.
- Eine Datei oder ein Verzeichnis erbt den Sicherheitsstil des übergeordneten FlexVol volume oder qtree.

SMB-Sicherheitsstile auf ONTAP SVM Root-Volumes konfigurieren

Der Sicherheitsstil des Root-Volumes der Storage Virtual Machine (SVM) wird konfiguriert, um die Art der Berechtigungen für Daten auf dem Root-Volume der SVM festzulegen.

Schritte

1. Der `vserver create`Befehl mit dem `-rootvolume-security-style`Parameter dient zur Definition des Sicherheitsstils.

   Die möglichen Optionen für den Sicherheitsstil des Root-Volumes sind `unix`, `ntfs` oder `mixed`.

2. Anzeige und Überprüfung der Konfiguration, einschließlich des Sicherheitsstils des Root-Volumes der erstellten SVM: `vserver show -vserver` *`vserver_name`*

SMB-Sicherheitsstile auf ONTAP FlexVol Volumes konfigurieren

Der Sicherheitsstil des FlexVol volume wird konfiguriert, um die Art der Berechtigungen festzulegen, die für Daten auf FlexVol volumes der Storage Virtual Machine (SVM) verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn das FlexVol Volume…	Verwenden Sie den Befehl…
Existiert noch nicht	`volume create` und den `-security-style` Parameter zur Angabe des Sicherheitsstils einschließen.
Existiert bereits	`volume modify` und den `-security-style` Parameter zur Angabe des Sicherheitsstils einschließen.

   Die möglichen Optionen für den FlexVol volume-Sicherheitsstil sind `unix`, `ntfs`, oder `mixed`.

   Wenn beim Erstellen eines FlexVol volume kein Sicherheitsstil angegeben wird, übernimmt das Volume den Sicherheitsstil des Stammvolumes.

   Weitere Informationen zu den `volume create` oder `volume modify` Befehlen finden sich unter "Logische Speicherverwaltung".

2. Um die Konfiguration einschließlich des Sicherheitsstils des von Ihnen erstellten FlexVol Volumes anzuzeigen, ist folgender Befehl einzugeben:

```
volume show -volume volume_name -instance
```

SMB-Sicherheitsstile auf ONTAP Qtrees konfigurieren

Der Sicherheitsstil des Qtree-Volumes wird konfiguriert, um die Art der Berechtigungen festzulegen, die für Daten auf Qtrees verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der Qtree…	Verwenden Sie den Befehl…
Existiert noch nicht	`volume qtree create` und den `-security -style` Parameter zur Angabe des Sicherheitsstils einschließen.
Existiert bereits	`volume qtree modify` und den `-security -style` Parameter zur Angabe des Sicherheitsstils einschließen.

   Die möglichen Optionen für den Qtree-Sicherheitsstil sind `unix`, `ntfs` oder `mixed`.

   Wenn beim Erstellen eines Qtree kein Sicherheitsstil angegeben wird, ist der Standard-Sicherheitsstil `mixed`.

   Weitere Informationen zu den `volume qtree create` oder `volume qtree modify` Befehlen finden sich unter "Logische Speicherverwaltung".

2. Um die Konfiguration, einschließlich des Sicherheitsstils des von Ihnen erstellten Qtrees, anzuzeigen, ist folgender Befehl einzugeben: `volume qtree show -qtree qtree_name -instance`

Copyright-Informationen

Copyright © 2026 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, BEISPIELHAFTE 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 IRGENDEINER 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.