



Einfluss der Sicherheitsstile auf den Datenzugriff

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

- Einfluss der Sicherheitsstile auf den Datenzugriff 1
 - Was die Sicherheitsstile und ihre Auswirkungen sind 1
 - Wo und wann Sicherheitsstile eingestellt werden sollen 2
 - Entscheiden Sie, welchen Sicherheitsstil auf SVMs verwendet werden soll 2
 - Wie funktioniert die Vererbung des Sicherheitsstils 3
 - Wie ONTAP UNIX-Berechtigungen bewahrt 3
 - Verwalten Sie UNIX-Berechtigungen über die Registerkarte Windows-Sicherheit 3

Einfluss der Sicherheitsstile auf den Datenzugriff

Was die Sicherheitsstile und ihre Auswirkungen sind

Es gibt vier verschiedene Sicherheitsarten: UNIX, NTFS, gemischt und vereinheitlicht. Jeder Sicherheitsstil hat unterschiedliche Auswirkungen auf den Umgang mit Berechtigungen für Daten. Sie müssen die verschiedenen Effekte verstehen, um sicherzustellen, dass Sie den entsprechenden Sicherheitsstil für Ihre Zwecke auswählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht bestimmen, welche Client-Typen auf Daten zugreifen können oder nicht. Sicherheitsstile bestimmen nur die Art der Berechtigungen, die ONTAP zur Kontrolle des Datenzugriffs verwendet, und welche Clienttypen diese Berechtigungen ändern können.

Wenn ein Volume beispielsweise UNIX-Sicherheitsstil verwendet, können SMB-Clients aufgrund der Multiprotokollart von ONTAP weiterhin auf Daten zugreifen (sofern sie sich ordnungsgemäß authentifizieren und autorisieren). 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	Dadurch effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
UNIX	NFS	Bits im NFSv3 Modus	UNIX	NFS und SMB
NFSv4.x ACLs	UNIX	NTFS	SMB	NTFS-ACLs
NTFS	Gemischt	NFS oder SMB	Bits im NFSv3 Modus	UNIX
NFSv4.x ACLs	UNIX	NTFS-ACLs	NTFS	Virtualisierung
NFS oder SMB	Bits im NFSv3 Modus	UNIX	NFSv4.1 ACLs	UNIX
NTFS-ACLs	NTFS	Unified (nur für Infinite Volumes, in ONTAP 9.4 und älteren Versionen.)	NFS oder SMB	Bits im NFSv3 Modus
Unix	NFSv4.1 ACLs			NTFS-ACLs

FlexVol Volumes unterstützen UNIX, NTFS und verschiedene Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder vereinheitlicht ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil auf individueller Basis festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modus-Bits. 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 Unified Security-Stil ist nur mit Infinite Volumes verfügbar, die in ONTAP 9.5 und neueren Versionen nicht mehr unterstützt werden. Weitere Informationen finden Sie unter ["Das Management von FlexGroup Volumes – Überblick"](#).

Ab ONTAP 9.2 beginnt der `show-effective-permissions` Parameter für das `vserver security file-directory` Mit Befehl können Sie effektive Berechtigungen anzeigen, die einem Windows- oder UNIX-Benutzer im angegebenen Datei- oder Ordnerpfad gewährt werden. Darüber hinaus der optionale Parameter `-share-name` Ermöglicht Ihnen die Anzeige der effektiven Freigabeberechtigung.



ONTAP legt zunächst einige Standarddateiberechtigungen fest. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in UNIX-, gemischten und Unified Security-Volumes UNIX und der effektive Berechtigungstyp UNIX Mode Bits (0755, sofern nicht anders angegeben), bis er von einem Client gemäß dem Standardsicherheitsstil konfiguriert wird. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in NTFS-Sicherheitsstil-Volumes NTFS und hat eine ACL, die allen die vollständige Kontrolle erlaubt.

Wo und wann Sicherheitsstile eingestellt werden sollen

Sicherheitsstile können auf FlexVol Volumes (Root-Volumes oder Daten-Volumes) und qtrees festgelegt werden. Sicherheitsstile können zum Zeitpunkt der Erstellung manuell eingestellt, automatisch geerbt oder zu einem späteren Zeitpunkt geändert werden.

Entscheiden Sie, welchen Sicherheitsstil auf SVMs verwendet werden soll

Um zu entscheiden, welchen Sicherheitsstil auf einem Volume verwendet werden soll, sollten Sie zwei Faktoren berücksichtigen. Der Hauptfaktor ist die Art des Administrators, der das Dateisystem verwaltet. Sekundär ist die Art des Benutzers oder Service, der auf die Daten des Volume zugreift.

Wenn Sie den Sicherheitsstil auf einem Volume konfigurieren, sollten Sie die Anforderungen Ihrer Umgebung berücksichtigen, um sicherzustellen, dass Sie den besten Sicherheitsstil wählen und Probleme beim Management von Berechtigungen vermeiden. Die folgenden Überlegungen helfen Ihnen bei der Auswahl:

Sicherheitsstil	Wählen Sie aus, ob...
UNIX	<ul style="list-style-type: none">• Das Dateisystem wird von einem UNIX-Administrator verwaltet.• Die Mehrheit der Benutzer sind NFS Clients.• Eine Anwendung, die auf die Daten zugreift, verwendet einen UNIX-Benutzer als Dienstkonto.
NTFS	<ul style="list-style-type: none">• Das Dateisystem wird von einem Windows-Administrator verwaltet.• Die Mehrheit der Benutzer sind SMB-Clients.• Eine Anwendung, die auf die Daten zugreift, verwendet einen Windows-Benutzer als Dienstkonto.

Sicherheitsstil	Wählen Sie aus, ob...
Gemischt	Das Filesystem wird sowohl von UNIX- als auch von Windows-Administratoren gemanagt, und die Benutzer bestehen sowohl aus NFS- als auch SMB-Clients.

Wie funktioniert die Vererbung des Sicherheitsstils

Wenn Sie beim Erstellen eines neuen FlexVol Volumes oder eines qtree nicht den Sicherheitsstil festlegen, übernimmt dieser seinen Sicherheitsstil auf unterschiedliche Weise.

Sicherheitsstile werden auf folgende Weise vererbt:

- Ein FlexVol Volume erbt den Sicherheitsstil des Root-Volumes seiner enthaltenen SVM.
- Ein qtree übernimmt den Sicherheitsstil seines enthaltenen FlexVol Volume.
- Eine Datei oder ein Verzeichnis erbt den Sicherheitsstil, den sie FlexVol Volume oder qtree enthält.

Wie ONTAP UNIX-Berechtigungen bewahrt

Wenn Dateien in einem FlexVol-Volume mit derzeit UNIX-Berechtigungen von Windows-Anwendungen bearbeitet und gespeichert werden, kann ONTAP die UNIX-Berechtigungen beibehalten.

Wenn Anwendungen auf Windows-Clients Dateien bearbeiten und speichern, lesen sie die Sicherheitseinstellungen der Datei, erstellen eine neue temporäre Datei, wenden diese Eigenschaften auf die temporäre Datei an und geben der temporären Datei dann den ursprünglichen Dateinamen an.

Wenn Windows-Clients eine Abfrage für die Sicherheitseigenschaften durchführen, erhalten sie eine konstruierte ACL, die genau die UNIX-Berechtigungen repräsentiert. Der einzige Zweck dieser aufgebauten ACL besteht darin, die UNIX-Berechtigungen der Datei beizubehalten, da Dateien von Windows-Anwendungen aktualisiert werden, um sicherzustellen, dass die resultierenden Dateien dieselben UNIX-Berechtigungen haben. ONTAP legt keine NTFS-ACLs mithilfe der konstruierten ACL fest.

Verwalten Sie UNIX-Berechtigungen über die Registerkarte Windows-Sicherheit

Wenn Sie UNIX-Berechtigungen von Dateien oder Ordnern in gemischten Volumes oder qtrees auf SVMs manipulieren möchten, können Sie auf Windows-Clients die Registerkarte „Sicherheit“ verwenden. Alternativ können Sie Anwendungen verwenden, die Windows ACLs abfragen und festlegen können.

- Ändern der UNIX-Berechtigungen

Mithilfe der Registerkarte Windows Security können Sie UNIX Berechtigungen für ein Volume oder einen qtree im gemischten Sicherheitsstil anzeigen und ändern. Wenn Sie die Windows-Hauptregisterkarte verwenden, um UNIX-Berechtigungen zu ändern, müssen Sie zuerst den vorhandenen ACE entfernen,

den Sie bearbeiten möchten (dadurch werden die Modusbits auf 0 gesetzt), bevor Sie Ihre Änderungen vornehmen. Alternativ können Sie den erweiterten Editor verwenden, um Berechtigungen zu ändern.

Bei Verwendung von Modusberechtigungen können Sie die Modusberechtigungen für die angegebene UID, GID und andere (alle anderen mit einem Konto auf dem Computer) direkt ändern. Wenn die angezeigte UID beispielsweise r-x-Berechtigungen hat, können Sie die UID-Berechtigungen in rwx ändern.

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

Sie können die Registerkarte Windows Security verwenden, um UNIX Sicherheitsobjekte durch Windows-Sicherheitsobjekte auf einem Volume mit gemischtem Sicherheitsstil oder qtree zu ersetzen, wobei die Dateien und Ordner einen effektiven UNIX-Sicherheitsstil haben.

Sie müssen zuerst alle aufgeführten UNIX-Berechtigungseinträge entfernen, bevor Sie sie durch die gewünschten Windows-Benutzer- und Gruppenobjekte ersetzen können. Anschließend können Sie NTFS-basierte ACLs auf den Windows-Benutzerobjekten konfigurieren. Indem Sie alle UNIX-Sicherheitsobjekte entfernen und nur Windows-Benutzer und -Gruppen zu einer Datei oder einem Ordner in einem gemischten Volume oder qtree hinzufügen, ändern Sie den effektiven Sicherheitsstil auf der Datei oder dem Ordner von UNIX auf NTFS.

Wenn Sie die Berechtigungen für einen Ordner ändern, ist das Windows-Standardverhalten, diese Änderungen auf alle Unterordner und Dateien zu übertragen. Daher müssen Sie die Ausbreitungsmöglichkeit auf die gewünschte Einstellung ändern, wenn Sie keine Änderung des Sicherheitsstils auf alle untergeordneten Ordner, Unterordner und Dateien übertragen möchten.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.