Managen Sie, wie Dateisicherheit SMB-Clients für UNIX-Sicherheitsdaten präsentiert wird

ONTAP 9

NetApp
September 12, 2024

Inhalt

Managen Sie, wie Dateisicherheit SMB-Clients für UNIX-Sicherheitsdaten präsentiert wird

Managen Sie die Dateisicherheit für SMB-Clients in der Übersicht über die Daten im UNIX-Sicherheitsstil

Sie können auswählen, wie Sie die Dateisicherheit SMB-Clients für UNIX-Sicherheitsdaten bereitstellen möchten, indem Sie die Präsentation von NTFS ACLs für SMB-Clients aktivieren oder deaktivieren. Jede Einstellung bietet Vorteile, die Sie verstehen sollten, die für Ihre geschäftlichen Anforderungen am besten geeignete Einstellung auszuwählen.

Standardmäßig stellt ONTAP SMB-Clients UNIX-Berechtigungen auf UNIX-Volumes im Sicherheitsstil als NTFS-ACLs zur Verfügung. Es gibt Szenarien, in denen dies wünschenswert ist, einschließlich:

- Sie möchten UNIX-Berechtigungen anzeigen und bearbeiten, indem Sie die Registerkarte **Sicherheit** im Feld Windows-Eigenschaften verwenden.

  Sie können keine Berechtigungen von einem Windows-Client ändern, wenn der Vorgang vom UNIX-System nicht erlaubt ist. Beispielsweise können Sie den Eigentümer einer Datei nicht ändern, da das UNIX-System diesen Vorgang nicht zulässt. Diese Einschränkung verhindert, dass SMB-Clients UNIX-Berechtigungen für die Dateien und Ordner umgehen.

- Benutzer bearbeiten und speichern Dateien auf dem UNIX-Security-Style-Volume unter Verwendung bestimmter Windows-Anwendungen, zum Beispiel Microsoft Office, wo ONTAP die UNIX-Berechtigungen während des Speichervorgangs erhalten muss.
- Es gibt bestimmte Windows-Anwendungen in Ihrer Umgebung, die damit rechnen, NTFS ACLs über Dateien zu lesen, die sie verwenden.

Unter bestimmten Umständen möchten Sie die Darstellung von UNIX Berechtigungen als NTFS ACLs deaktivieren. Wenn diese Funktion deaktiviert ist, stellt ONTAP den SMB-Clients SicherheitsVolumes im UNIX-Stil als FAT-Volumes zur Verfügung. Es gibt spezifische Gründe, warum Sie UNIX Security-Style Volumes als FAT Volumes für SMB-Clients präsentieren möchten:

- Sie ändern nur UNIX-Berechtigungen, indem Sie Mounts auf UNIX-Clients verwenden.

  Die Registerkarte Sicherheit ist nicht verfügbar, wenn ein UNIX-Volume nach Sicherheitsstil auf einem SMB-Client zugeordnet ist. Das zugeordnete Laufwerk scheint mit dem FAT-Dateisystem formatiert zu sein, das keine Dateiberechtigungen hat.

- Sie verwenden Anwendungen über SMB, die NTFS-ACLs auf Dateien und Ordner festlegen, die auf Dateien und Ordner zugegriffen werden kann. Dies kann fehlschlagen, wenn sich die Daten auf UNIX-Volumes befinden.

  Wenn ONTAP das Volumen als FAT meldet, versucht die Anwendung nicht, eine ACL zu ändern.

Verwandte Informationen

Konfiguration von Sicherheitsstilen auf FlexVol Volumes

Konfigurieren von Sicherheitsstilen auf qtrees

Aktivieren oder deaktivieren Sie die Darstellung von NTFS ACLs für UNIX-Sicherheitsdaten

Sie können die Präsentation von NTFS ACLs für SMB-Clients für UNIX-Sicherheitsdaten aktivieren oder deaktivieren (UNIX-Volumes im Sicherheitsstil und Volumes im gemischten Sicherheitsstil mit effektiver Sicherheit von UNIX).

Über diese Aufgabe

Wenn Sie diese Option aktivieren, stellt ONTAP SMB-Clients Dateien und Ordner auf Volumes mit effektivem UNIX-Sicherheitsstil als NTFS-ACLs vor. Wenn Sie diese Option deaktivieren, werden die Volumes SMB-Clients als FAT Volumes angezeigt. Der Standardwert ist, um NTFS ACLs an SMB-Clients zu präsentieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Konfigurieren Sie die Einstellung der UNIX NTFS ACL-Option: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Vergewissern Sie sich, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver vserver_name`
4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

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.