Verwenden Sie Optionen zum Anpassen von SMB-Servern

ONTAP 9

NetApp
September 12, 2024

Inhalt

Verwenden Sie Optionen zum Anpassen von SMB-Servern

Verfügbare SMB-Server-Optionen

Es ist nützlich zu wissen, welche Optionen zur Verfügung stehen, wenn Sie die Anpassung des SMB Servers in Betracht ziehen. Einige Optionen sind zwar allgemein auf dem SMB-Server einsetzbar, jedoch werden mehrere zur Aktivierung und Konfiguration spezifischer SMB-Funktionen verwendet. Die Optionen für SMB-Server werden über das gesteuert `vserver cifs options modify` Option.

In der folgenden Liste werden die SMB-Server-Optionen angegeben, die auf der Administratorberechtigungsebene verfügbar sind:

- **Konfiguration des SMB Session-Timeout-Wertes**

  Wenn Sie diese Option konfigurieren, können Sie die Anzahl der Sekunden für die Leerlaufzeit festlegen, bevor eine SMB-Sitzung getrennt wird. Eine leere Sitzung ist eine Sitzung, in der ein Benutzer keine Dateien oder Verzeichnisse auf dem Client geöffnet hat. Der Standardwert ist 900 Sekunden.

- **Konfigurieren des UNIX-Standardbenutzers**

  Wenn Sie diese Option konfigurieren, können Sie den UNIX-Standardbenutzer angeben, den der SMB-Server verwendet. ONTAP erstellt automatisch einen Standardbenutzer mit dem Namen „`pcuser`“ (mit einer UID von 65534), erstellt eine Gruppe mit dem Namen „`pcuser`“ (mit einer GID von 65534) und fügt den Standardbenutzer der Gruppe „`pcuser`“ hinzu. Wenn Sie einen SMB-Server erstellen, konfiguriert ONTAP „`pcuser`“ automatisch als Standard-UNIX-Benutzer.

- **Konfigurieren des UNIX-Gastbenutzers**

  Wenn Sie diese Option konfigurieren, können Sie den Namen eines UNIX-Benutzers angeben, dem Benutzer zugewiesen werden, die sich von nicht vertrauenswürdigen Domänen aus anmelden, sodass ein Benutzer von einer nicht vertrauenswürdigen Domäne aus eine Verbindung zum SMB-Server herstellen kann. Standardmäßig ist diese Option nicht konfiguriert (es gibt keinen Standardwert). Daher ist die Standardeinstellung, dass Benutzer aus nicht vertrauenswürdigen Domänen keine Verbindung zum SMB-Server herstellen können.

- **Aktivieren oder Deaktivieren der Ausführung der Lesezuteilung für Mode-Bits**

  Wenn Sie diese Option aktivieren oder deaktivieren, können Sie angeben, ob SMB-Clients erlauben sollen, ausführbare Dateien mit UNIX-Modus-Bits auszuführen, auf die sie Lesezugriff haben, auch wenn das UNIX-Executable-Bit nicht eingestellt ist. Diese Option ist standardmäßig deaktiviert.

- **Aktivieren oder Deaktivieren der Fähigkeit, schreibgeschützte Dateien von NFS-Clients zu löschen**

  Wenn Sie diese Option aktivieren oder deaktivieren, wird festgelegt, ob NFS-Clients Dateien oder Ordner mit dem Schreibschutzattribut löschen dürfen. NTFS delete Semantik erlaubt nicht das Löschen einer Datei oder eines Ordners, wenn das Attribut nur Lesen festgelegt ist. UNIX delete Semantik ignoriert das schreibgeschützte Bit und verwendet stattdessen die Berechtigungen des übergeordneten Verzeichnisses, um zu bestimmen, ob eine Datei oder ein Ordner gelöscht werden kann. Die Standardeinstellung ist `disabled`, Die in NTFS zu löschen Semantik führt.

- **Konfigurieren von Windows Internet Name Service Server-Adressen**

  Wenn Sie diese Option konfigurieren, können Sie eine Liste von WINS-Serveradressen (Windows Internet Name Service) als kommagetrennte Liste angeben. Sie müssen IPv4-Adressen angeben. IPv6-Adressen werden nicht unterstützt. Es gibt keinen Standardwert.

In der folgenden Liste werden die SMB-Serveroptionen angegeben, die auf der erweiterten Berechtigungsebene verfügbar sind:

- **Gewährung von UNIX-Gruppenberechtigungen für CIFS-Benutzer**

  Durch die Konfiguration dieser Option wird festgelegt, ob der eingehende CIFS-Benutzer, der nicht der Eigentümer der Datei ist, die Gruppenberechtigung erhalten kann. Wenn der CIFS-Benutzer nicht der Besitzer der UNIX-Sicherheitsdatei ist und dieser Parameter auf festgelegt ist `true`, Dann wird die Gruppenberechtigung für die Datei erteilt. Wenn der CIFS-Benutzer nicht der Besitzer der UNIX-Sicherheitsdatei ist und dieser Parameter auf festgelegt ist `false`, Dann sind die normalen UNIX-Regeln für die Erteilung der Dateiberechtigung. Dieser Parameter gilt für UNIX-Dateien im Sicherheitsstil, die als Berechtigungen festgelegt sind `mode bits` Und gilt nicht für Dateien mit dem NTFS oder NFSv4-Sicherheitsmodus. Die Standardeinstellung ist `false`.

- **Aktivieren oder Deaktivieren von SMB 1.0**

  SMB 1.0 ist auf einer SVM, für die in ONTAP 9.3 ein SMB-Server erstellt wurde, standardmäßig deaktiviert.

  > Ab ONTAP 9.3 ist SMB 1.0 für neue in ONTAP 9.3 erstellte SMB-Server standardmäßig deaktiviert. Sie sollten so bald wie möglich auf eine neuere SMB-Version migrieren, um sich auf Sicherheits- und Compliance-Verbesserungen vorzubereiten. Genaue Informationen erhalten Sie bei Ihrem NetApp Ansprechpartner.

- **Aktivieren oder Deaktivieren von SMB 2.x**

  SMB 2.0 ist die minimale SMB-Version, die LIF Failover unterstützt. Wenn Sie SMB 2.x deaktivieren, deaktiviert ONTAP auch SMB 3.X automatisch

  SMB 2.0 wird nur auf SVMs unterstützt. Die Option ist bei SVMs standardmäßig aktiviert

- **Aktivieren oder Deaktivieren von SMB 3.0**

  SMB 3.0 ist die minimale SMB-Version, die kontinuierlich verfügbare Freigaben unterstützt. Windows Server 2012 und Windows 8 sind die Mindestversionen von Windows, die SMB 3.0 unterstützen.

  SMB 3.0 wird nur auf SVMs unterstützt. Die Option ist bei SVMs standardmäßig aktiviert

- **Aktivieren oder Deaktivieren von SMB 3.1**

  Windows 10 ist die einzige Windows Version, die SMB 3.1 unterstützt.

  SMB 3.1 wird nur auf SVMs unterstützt. Die Option ist bei SVMs standardmäßig aktiviert

- **Aktivieren oder Deaktivieren von ODX Copy Offload**

  Der ODX Copy Offload wird automatisch von Windows Clients genutzt, die diese unterstützen. Diese Option ist standardmäßig aktiviert.

- **Aktivieren oder Deaktivieren des Direct-Copy-Mechanismus für ODX Copy Offload**

  Der Direct-Copy-Mechanismus erhöht die Performance für den Offload, wenn Windows Clients versuchen, die Quelldatei einer Kopie in einem Modus zu öffnen, der verhindert, dass die Datei während des Kopiervorgangs geändert wird. Standardmäßig ist der Mechanismus für die direkte Kopie aktiviert.

- **Aktivieren oder Deaktivieren automatischer Knotenempfehlungen**

  Bei automatischen Node-Empfehlungen verweist der SMB-Server Clients automatisch auf eine lokale Daten-LIF auf den Node, der die Daten hostet, auf die über die angeforderte Freigabe zugegriffen wird.

- **Aktivieren oder Deaktivieren von Exportrichtlinien für SMB**

  Diese Option ist standardmäßig deaktiviert.

- **Aktivieren oder Deaktivieren der Verwendung von Verbindungspunkten als Parsen-Punkte**

  Wenn diese Option aktiviert ist, legt der SMB-Server SMB-Clients Verbindungspunkte als Analysepunkte bereit. Diese Option ist nur für SMB 2.x- oder SMB 3.0-Verbindungen gültig. Diese Option ist standardmäßig aktiviert.

  Diese Option wird nur auf SVMs unterstützt. Die Option ist bei SVMs standardmäßig aktiviert

- **Konfiguration der Anzahl der maximalen gleichzeitigen Operationen pro TCP-Verbindung**

  Der Standardwert ist 255.

- **Aktivieren oder Deaktivieren der Funktionalität von lokalen Windows-Benutzern und -Gruppen**

  Diese Option ist standardmäßig aktiviert.

- **Aktivieren oder Deaktivieren der Authentifizierung von lokalen Windows-Benutzern**

  Diese Option ist standardmäßig aktiviert.

- **Aktivieren oder Deaktivieren der VSS-Schattenkopiefunktion**

  ONTAP nutzt die Funktionalität für Schattenkopien, um Remote-Backups von Daten durchzuführen, die mit Hyper-V over SMB gespeichert sind.

  Diese Option wird nur auf SVMs und nur für Hyper-V über SMB-Konfigurationen unterstützt. Die Option ist bei SVMs standardmäßig aktiviert

- **Konfigurieren der Verzeichnistiefe der Schattenkopie**

  Wenn Sie diese Option konfigurieren, können Sie die maximale Tiefe von Verzeichnissen festlegen, auf denen bei Verwendung der Schattenkopiefunktion Schattenkopien erstellt werden sollen.

  Diese Option wird nur auf SVMs und nur für Hyper-V über SMB-Konfigurationen unterstützt. Die Option ist bei SVMs standardmäßig aktiviert

- **Aktivieren oder Deaktivieren von Multidomain-Suchfunktionen für Namenszuordnungen**

  Wenn aktiviert, sucht ONTAP, wenn ein UNIX-Benutzer einem Windows-Domänenbenutzer über einen Platzhalter (*) im Domain-Teil des Windows-Benutzernamens (z. B. *\joe) zugeordnet wird, in allen Domänen nach dem angegebenen Benutzer mit bidirektionalen Vertrauensstellungen für die Home-

Domain. Die Home-Domäne ist die Domäne, die das Computerkonto des SMB-Servers enthält.

Als Alternative zum Durchsuchen aller bidirektional vertrauenswürdigen Domänen können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren. Wenn diese Option aktiviert ist und eine bevorzugte Liste konfiguriert ist, wird die bevorzugte Liste verwendet, um Suchen zur Zuordnung von Namen mit mehreren Domänen durchzuführen.

Standardmäßig werden Suchvorgänge für die Zuordnung von Mehrfachdomänen aktiviert.

- **Konfigurieren der Sektorgröße des Dateisystems**

  Wenn Sie diese Option konfigurieren, können Sie die Größe des Dateisystemsektors in Bytes konfigurieren, die ONTAP an SMB-Clients meldet. Für diese Option gibt es zwei gültige Werte: `4096` Und `512`. Der Standardwert ist `4096`. Möglicherweise müssen Sie diesen Wert auf einstellen `512` Wenn die Windows-Anwendung nur eine Sektorgröße von 512 Byte unterstützt.

- **Aktivieren oder Deaktivieren der Dynamic Access Control**

  Wenn diese Option aktiviert wird, können Sie Objekte auf dem SMB-Server mithilfe von Dynamic Access Control (DAC) sichern. Dazu gehören Prüfungen zum Staging von zentralen Zugriffsrichtlinien und Group Policy Objects zur Implementierung zentraler Zugriffsrichtlinien. Die Option ist standardmäßig deaktiviert.

  Diese Option wird nur auf SVMs unterstützt.

- **Festlegen der Zugriffsbeschränkungen für nicht authentifizierte Sitzungen (anonym beschränken)**

  Durch das Festlegen dieser Option wird festgelegt, welche Zugriffsbeschränkungen für nicht authentifizierte Sitzungen gelten. Die Einschränkungen gelten für anonyme Benutzer. Standardmäßig gibt es keine Zugriffsbeschränkungen für anonyme Benutzer.

- **Aktivieren oder Deaktivieren der Präsentation von NTFS ACLs auf Volumes mit UNIX effektive Sicherheit (UNIX Security-Style Volumes oder gemischte Security-Style Volumes mit UNIX Effective Security)**

  Wenn Sie diese Option aktivieren oder deaktivieren, wird bestimmt, wie die Dateisicherheit auf Dateien und Ordnern mit UNIX-Sicherheit SMB-Clients angezeigt wird. Wenn aktiviert, präsentiert ONTAP Dateien und Ordner in Volumes mit UNIX-Sicherheit für SMB-Clients als NTFS-Dateisicherheit mit NTFS-ACLs. Wenn deaktiviert, präsentiert ONTAP Volumes mit UNIX-Sicherheit als FAT-Volumes, ohne Dateisicherheit. Standardmäßig werden Volumes als NTFS-Dateisicherheit mit NTFS-ACLs präsentiert.

- **Aktivieren oder Deaktivieren der SMB Fake Open-Funktionalität**

  Durch die Aktivierung dieser Funktion wird die Performance von SMB 2.x und SMB 3.0 verbessert, da beim Abfragen von Attributinformationen zu Dateien und Verzeichnissen die Art und Weise optimiert wird, wie ONTAP offene und Abschlussanfragen erstellt. Standardmäßig ist die SMB Fake Open-Funktion aktiviert. Diese Option ist nur für Verbindungen nützlich, die mit SMB 2.x oder höher hergestellt werden.

- **Aktivieren oder Deaktivieren der UNIX-Erweiterungen**

  Wenn Sie diese Option aktivieren, werden UNIX-Erweiterungen auf einem SMB-Server aktiviert. UNIX-Erweiterungen ermöglichen es, die Sicherheit im POSIX-/UNIX-Stil über das SMB-Protokoll anzuzeigen. Diese Option ist standardmäßig deaktiviert.

  Wenn Sie UNIX-basierte SMB-Clients, z. B. Mac OSX-Clients, in Ihrer Umgebung haben, sollten Sie UNIX-Erweiterungen aktivieren. Durch die Aktivierung von UNIX-Erweiterungen kann der SMB-Server POSIX/UNIX-Sicherheitsinformationen über SMB an den UNIX-basierten Client übertragen, wodurch die

Sicherheitsinformationen in die POSIX/UNIX-Sicherheit übersetzt werden.

- **Unterstützung für Kurznamensuchen aktivieren oder deaktivieren**

  Wenn Sie diese Option aktivieren, kann der SMB-Server Suchen nach Kurznamen durchführen. Eine Suchabfrage mit aktivierter Option versucht, 8.3 Dateinamen zusammen mit langen Dateinamen zu entsprechen. Der Standardwert für diesen Parameter ist `false`.

- **Aktivieren oder Deaktivieren der Unterstützung für automatische Werbung von DFS-Funktionen**

  Durch Aktivieren oder Deaktivieren dieser Option wird festgelegt, ob SMB-Server DFS-Funktionen automatisch an SMB 2.x- und SMB 3.0-Clients weitergeben, die eine Verbindung zu Freigaben herstellen. ONTAP verwendet DFS-Empfehlungen bei der Implementierung von symbolischen Links für den SMB-Zugriff. Wenn diese Option aktiviert ist, gibt der SMB-Server immer DFS-Funktionen an, unabhängig davon, ob der symbolische Link-Zugriff aktiviert ist. Wenn diese Option deaktiviert ist, gibt der SMB-Server DFS-Funktionen nur an, wenn die Clients eine Verbindung zu Freigaben herstellen, bei denen der symbolische Link-Zugriff aktiviert ist.

- **Konfiguration der maximalen Anzahl von SMB Credits**

  Ab ONTAP 9.4 konfigurieren Sie den `-max-credits` Mit dieser Option können Sie die Anzahl der Credits begrenzen, die auf einer SMB-Verbindung gewährt werden sollen, wenn auf Clients und Servern SMB Version 2 oder höher ausgeführt wird. Der Standardwert ist 128.

- **Aktivieren oder Deaktivieren der Unterstützung für SMB Multichannel**

  Aktivieren der `-is-multichannel-enabled` Mit der Option in ONTAP 9.4 und neueren Versionen kann der SMB-Server mehrere Verbindungen für eine einzelne SMB-Sitzung herstellen, wenn entsprechende NICs auf dem Cluster und seinen Clients implementiert werden. Dadurch werden Durchsatz und Fehlertoleranz verbessert. Der Standardwert für diesen Parameter ist `false`.

  Wenn SMB Multichannel aktiviert ist, können Sie auch die folgenden Parameter angeben:

  - Die maximal zulässige Anzahl von Verbindungen pro Multichannel-Sitzung. Der Standardwert für diesen Parameter ist 32.
  - Die maximale Anzahl der pro Multichannel-Sitzung angekündigten Netzwerkschnittstellen. Der Standardwert für diesen Parameter ist 256.

SMB-Serveroptionen werden konfiguriert

Sie können SMB-Serveroptionen jederzeit konfigurieren, nachdem Sie einen SMB-Server auf einer Storage Virtual Machine (SVM) erstellt haben.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Optionen für SMB-Server konfigurieren…	Geben Sie den Befehl ein…
Auf der Administrator-Berechtigungsebene	`vserver cifs options modify -vserver` *`vserver_name options`*

Optionen für SMB-Server konfigurieren…	Geben Sie den Befehl ein…
Auf der Ebene der erweiterten Berechtigungen	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Weitere Informationen zum Konfigurieren von SMB-Serveroptionen finden Sie auf der man-Page für das `vserver cifs options modify` Befehl.

Konfigurieren Sie die Berechtigung UNIX-Gruppen für SMB-Benutzer gewähren

Sie können diese Option so konfigurieren, dass Gruppenberechtigungen für den Zugriff auf Dateien oder Verzeichnisse gewährt werden, selbst wenn der eingehende SMB-Benutzer nicht der Eigentümer der Datei ist.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Konfigurieren Sie die Berechtigung für die UNIX-Gruppe gewähren wie folgt:

Wenn Sie möchten	Geben Sie den Befehl ein
Aktivieren Sie den Zugriff auf die Dateien oder Verzeichnisse, um Gruppenberechtigungen zu erhalten, selbst wenn der Benutzer nicht Eigentümer der Datei ist	`vserver cifs options modify –grant-unix-group-perms-to-others true`
Deaktivieren Sie den Zugriff auf die Dateien oder Verzeichnisse, um Gruppenberechtigungen zu erhalten, selbst wenn der Benutzer nicht der Eigentümer der Datei ist	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. Vergewissern Sie sich, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Konfiguration von Zugriffsbeschränkungen für anonyme Benutzer

Standardmäßig kann ein anonymer, nicht authentifizierter Benutzer (auch bekannt als *Null-Benutzer*) auf bestimmte Informationen im Netzwerk zugreifen. Sie können eine SMB-Serveroption verwenden, um Zugriffsbeschränkungen für anonyme Benutzer zu konfigurieren.

Über diese Aufgabe

Der `-restrict-anonymous` Die SMB-Serveroption entspricht der `RestrictAnonymous` Registrierungseintrag in Windows.

Anonyme Benutzer können bestimmte Arten von Systeminformationen von Windows-Hosts im Netzwerk auflisten oder auflisten, einschließlich Benutzernamen und Details, Kontorichtlinien und Freigabenamen. Sie können den Zugriff für den anonymen Benutzer steuern, indem Sie eine der drei Einstellungen für Zugriffsbeschränkungen angeben:

Wert	Beschreibung
`no-restriction` (Standard)	Gibt keine Zugriffsbeschränkungen für anonyme Benutzer an.
`no-enumeration`	Gibt an, dass nur die Aufzählung für anonyme Benutzer beschränkt ist.
`no-access`	Gibt an, dass der Zugriff für anonyme Benutzer beschränkt ist.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Konfigurieren Sie die Einstellung anonyme beschränken: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
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`

Verwandte Informationen

Verfügbare SMB-Server-Optionen

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.