# SMB Server verwalten

ONTAP 9

NetApp
October 22, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/modify-servers-task.html on October 22, 2026. Always check docs.netapp.com for the latest.

# Inhalt


SMB Server verwalten . . . 1
ONTAP SMB-Server modifizieren . . . 1
Optionen zur Anpassung von SMB-Servern verwenden . . . 2
Verfügbare ONTAP SMB Serveroptionen . . . 2
ONTAP SMB-Serveroptionen konfigurieren . . . 7
Die UNIX-Gruppenberechtigung für ONTAP SMB-Benutzer konfigurieren . . . 7
ONTAP SMB-Zugriffsbeschränkungen für anonyme Benutzer konfigurieren . . . 8
Steuerung der Darstellung der Dateisicherheit für SMB-Clients bei UNIX-Sicherheitsstil-Daten . . . 9
Informationen zur Präsentation der ONTAP Dateisicherheit für SMB-Clients bei Daten im UNIX-Sicherheitsstil . . . 9
Die Darstellung von NTFS-ACLs für ONTAP SMB-Clients bei UNIX-Sicherheitsstil-Daten konfigurieren 10
Informationen zur Beibehaltung von UNIX-Berechtigungen für ONTAP SMB FlexVol Volumes . . . 10
Informationen zur Verwaltung von UNIX-Berechtigungen über die Registerkarte „Windows-Sicherheit“ für ONTAP SMB-Server . . . 10
ONTAP SMB Multichannel für optimale Leistung und Redundanz konfigurieren . . . 11
Standardzuordnung von Windows-Benutzern zu UNIX-Benutzern auf dem SMB-Server konfigurieren . . . 13
Standardmäßigen ONTAP SMB UNIX Benutzer konfigurieren . . . 13
Den Gast-ONTAP SMB UNIX-Benutzer konfigurieren . . . 15
Administratorgruppen dem ONTAP SMB-Stamm zuordnen . . . 16
Informationen darüber, welche Benutzertypen über ONTAP SMB-Sitzungen verbunden sind, anzeigen . . . 17
ONTAP Befehlsoptionen zur Begrenzung des übermäßigen Ressourcenverbrauchs von Windows Clients . . . 18
Die Client-Performance mit traditionellen und Lease-Oplocks verbessern . . . 19
Informationen zur Verbesserung der ONTAP SMB-Client-Performance mit traditionellen und Lease-Oplocks . . . 19
Informationen zu Überlegungen zum Datenverlust im ONTAP SMB-Cache beim Einsatz von Oplocks . . . 19
Oplocks beim Erstellen von ONTAP SMB-Freigaben aktivieren oder deaktivieren . . . 20
ONTAP Befehle zum Aktivieren oder Deaktivieren von Oplocks auf SMB-Volumes und Qtrees . . . 21
Oplocks auf bestehenden ONTAP SMB-Freigaben aktivieren oder deaktivieren . . . 22
ONTAP SMB Oplock-Status überwachen . . . 23
Gruppenrichtlinienobjekte auf SMB-Server anwenden . . . 25
Informationen zur Anwendung von Gruppenrichtlinienobjekten auf ONTAP SMB Servern . . . 25
Informationen zu unterstützten ONTAP SMB Gruppenrichtlinienobjekten . . . 26
ONTAP SMB-Server Anforderungen für Gruppenrichtlinienobjekte . . . 31
GPO-Unterstützung auf ONTAP SMB-Servern aktivieren oder deaktivieren . . . 31
Informationen zum Aktualisieren von Gruppenrichtlinienobjekten (GPOs) auf ONTAP SMB-Servern . . . 32
Manuelle Aktualisierung der GPO-Einstellungen auf ONTAP SMB Servern . . . 33
Informationen zu ONTAP SMB GPO-Konfigurationen . . . 34
Informationen zu ONTAP SMB eingeschränkten Gruppenrichtlinien (GPOs) anzeigen . . . 38
Informationen zu den zentralen Zugriffsrichtlinien von ONTAP SMB anzeigen . . . 40
Informationen zu den zentralen Zugriffsrichtlinienregeln von ONTAP SMB anzeigen . . . 42
ONTAP Befehle zur Verwaltung von Passwörtern für SMB-Server-Computerkonten . . . 44
Domänencontrollerverbindungen verwalten . . . 44

Informationen zu ONTAP SMB erkannten Servern . . . 44
ONTAP SMB-Server zurücksetzen und neu erkennen . . . 45
Verwaltung der ONTAP SMB Domain Controller-Erkennung . . . 46
Bevorzugte ONTAP SMB-Domänencontroller hinzufügen . . . 47
ONTAP Befehle zur Verwaltung bevorzugter SMB-Domänencontroller . . . 48
Verschlüsselte Verbindungen zu ONTAP SMB-Domänencontrollern aktivieren . . . 48
Null-Sitzungen ermöglichen den Zugriff auf Speicher in Nicht-Kerberos-Umgebungen. . . . 48
ONTAP SMB-Nullsitzungen ermöglichen den Zugriff auf Speicher in Nicht-Kerberos-Umgebungen . . . 48
Wie ONTAP SMB Speichersysteme Null-Session-Zugriff bereitstellen, wird erläutert. . . . 49
Null-Benutzern Zugriff auf ONTAP SMB-Dateisystemfreigaben gewähren . . . 49
NetBIOS-Aliase für SMB Server verwalten . . . 50
Informationen zur Verwaltung von NetBIOS-Aliasen für ONTAP SMB-Server . . . 51
NetBIOS-Aliaslisten zu ONTAP SMB-Servern hinzufügen . . . 51
NetBIOS-Aliase aus der Liste für ONTAP SMB-Server entfernen . . . 52
NetBIOS-Aliasliste für ONTAP SMB-Server . . . 52
Feststellen, ob ONTAP SMB-Clients über NetBIOS-Aliase verbunden sind . . . 53
Verschiedene SMB Serveraufgaben verwalten . . . 54
ONTAP SMB-Server stoppen oder starten . . . 55
ONTAP SMB-Server in andere Organisationseinheiten verschieben . . . 55
Die dynamische DNS-Domäne vor dem Verschieben von ONTAP SMB-Servern anpassen. . . . 56
ONTAP SMB SVMs mit Active Directory-Domänen verbinden . . . 56
Informationen zu ONTAP SMB NetBIOS über TCP-Verbindungen . . . 58
ONTAP Befehle zur Verwaltung von SMB Servern . . . 58
Den ONTAP SMB NetBios-Namensdienst aktivieren . . . 59
IPv6 für SMB-Zugriff und SMB-Dienste verwenden . . . 60
Informationen zu den ONTAP SMB-Anforderungen für IPv6 . . . 60
Informationen zur Unterstützung von IPv6 mit ONTAP SMB-Zugriff und CIFS-Services . . . 60
Es wird erläutert, wie ONTAP SMB-Server IPv6 verwenden, um eine Verbindung zu externen Servern herzustellen. . . . 62
IPv6 für ONTAP SMB Server aktivieren . . . 63
Informationen zum Deaktivieren von IPv6 für ONTAP SMB Server . . . 63
Überwachung und Anzeige von Informationen zu IPv6 ONTAP SMB-Sitzungen . . . 63

# SMB Server verwalten

## ONTAP SMB-Server modifizieren

Ein SMB-Server kann von einer Arbeitsgruppe in eine Active Directory Domäne, von einer Arbeitsgruppe in eine andere Arbeitsgruppe oder von einer Active Directory Domäne in eine Arbeitsgruppe mithilfe des `vserver cifs modify` Befehls verschoben werden.

**Über diese Aufgabe**

Sie können auch andere Attribute des SMB-Servers ändern, wie zum Beispiel den SMB-Servernamen und den administrativen Status. Weitere Informationen zu `vserver cifs modify` finden sich in der "ONTAP-Befehlsreferenz".

**Auswahlmöglichkeiten**

- Verschieben des SMB-Servers von einer Arbeitsgruppe in eine Active Directory Domäne:

  a. Der administrative Status des SMB-Servers wird auf `down` gesetzt.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Den SMB-Server von der Arbeitsgruppe in eine Active Directory Domäne verschieben: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  Um ein Active Directory Computerkonto für den SMB-Server zu erstellen, müssen der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen angegeben werden, um Computer zum `ou=`*`example`* `ou` Container innerhalb der *`example`*.com-Domäne hinzuzufügen.

  Ab ONTAP 9.7 kann Ihnen Ihr AD-Administrator als Alternative zu einem Namen und Passwort für ein privilegiertes Windows-Konto eine URI zu einer Keytab-Datei bereitstellen. Nach Erhalt der URI ist diese im `-keytab-uri` Parameter mit den `vserver cifs` Befehlen anzugeben.

- Verschieben des SMB-Servers von einer Arbeitsgruppe in eine andere Arbeitsgruppe:

  a. Der administrative Status des SMB-Servers wird auf `down` gesetzt.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Die Arbeitsgruppe für den SMB-Server ändern: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- Verschieben des SMB-Servers von einer Active Directory Domäne in eine Arbeitsgruppe:
  a. Der administrative Status des SMB-Servers wird auf `down` gesetzt.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Den SMB-Server aus der Active Directory Domäne in eine Arbeitsgruppe verschieben: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> Um in den Arbeitsgruppenmodus zu wechseln, müssen alle domänenbasierten Funktionen deaktiviert und deren Konfiguration automatisch vom System entfernt werden, einschließlich permanent verfügbarer Freigaben, Schattenkopien und AES. Domänenkonfigurierte Freigabe-ACLs wie „EXAMPLE.COM\userName“ funktionieren jedoch nicht ordnungsgemäß, können aber nicht von ONTAP entfernt werden. Diese Freigabe-ACLs sollten so bald wie möglich nach Abschluss des Befehls mithilfe externer Tools entfernt werden. Wenn AES aktiviert ist, kann es erforderlich sein, den Namen und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen anzugeben, um es in der Domäne „EXAMPLE.COM“ zu deaktivieren.

  - Andere Attribute lassen sich mit dem entsprechenden Parameter des `vserver cifs modify` Befehls ändern.

# Optionen zur Anpassung von SMB-Servern verwenden

## Verfügbare ONTAP SMB Serveroptionen

Es ist hilfreich, die verfügbaren Optionen zu kennen, wenn die Anpassung des SMB-Servers in Betracht gezogen wird. Obwohl einige Optionen für die allgemeine Verwendung auf dem SMB-Server vorgesehen sind, werden mehrere zur Aktivierung und Konfiguration spezifischer SMB-Funktionen verwendet. SMB-Serveroptionen werden mit der `vserver cifs options modify` Option gesteuert.

Die folgende Liste enthält die SMB-Serveroptionen, die auf Administratorebene verfügbar sind:

- **Konfigurieren des Zeitüberschreitungswerts für die SMB-Sitzung**

  Durch die Konfiguration dieser Option können Sie die Anzahl der Sekunden Leerlaufzeit festlegen, nach der eine SMB-Sitzung getrennt wird. Eine inaktive Sitzung ist eine Sitzung, in der ein Benutzer keine Dateien oder Verzeichnisse auf dem Client geöffnet hat. Der Standardwert beträgt 900 Sekunden.

- **Konfigurieren des Standard-UNIX-Benutzers**

  Durch die Konfiguration dieser Option kann der Standard-UNIX-Benutzer festgelegt werden, den der SMB-Server verwendet. ONTAP erstellt automatisch einen Standardbenutzer namens „`pcuser`“ (mit der UID 65534), erstellt eine Gruppe namens „`pcuser`“ (mit der GID 65534) und fügt den Standardbenutzer der Gruppe „`pcuser`“ hinzu. Beim Erstellen eines SMB-Servers wird „`pcuser`“ von ONTAP automatisch als

Standard-UNIX-Benutzer konfiguriert.

- **Konfiguration des Gast-UNIX-Benutzers**

  Durch die Konfiguration dieser Option kann der Name eines UNIX-Benutzers festgelegt werden, dem Benutzer zugeordnet werden, die sich aus nicht vertrauenswürdigen Domänen anmelden. Dadurch wird es einem Benutzer aus einer nicht vertrauenswürdigen Domäne ermöglicht, eine Verbindung zum SMB-Server herzustellen. Standardmäßig ist diese Option nicht konfiguriert (es gibt keinen Standardwert), daher ist es standardmäßig nicht zulässig, dass Benutzer aus nicht vertrauenswürdigen Domänen eine Verbindung zum SMB-Server herstellen.

- **Aktivieren oder Deaktivieren der Ausführung der Leseberechtigung für Modusbits**

  Durch Aktivieren oder Deaktivieren dieser Option kann festgelegt werden, ob SMB-Clients ausführbare Dateien mit UNIX-Modusbits ausführen dürfen, auf die sie Lesezugriff haben, selbst wenn das UNIX-Ausführungsbit nicht gesetzt ist. Diese Option ist standardmäßig deaktiviert.

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

  Durch Aktivieren oder Deaktivieren dieser Option wird festgelegt, ob NFS-Clients das Löschen von Dateien oder Ordnern mit gesetztem Schreibschutz-Attribut erlauben. Die NTFS-Löschsemantik erlaubt das Löschen einer Datei oder eines Ordners mit gesetztem Schreibschutz-Attribut nicht. Die UNIX-Löschsemantik ignoriert das Schreibschutz-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`, was der NTFS-Löschsemantik entspricht.

- **Konfiguration der Windows Internet Name Service Serveradressen**

  Durch die Konfiguration dieser Option können Sie eine Liste von Windows Internet Name Service (WINS) Serveradressen als kommagetrennte Liste angeben. Sie müssen IPv4-Adressen angeben. IPv6-Adressen werden nicht unterstützt. Es gibt keinen Standardwert.

Die folgende Liste enthält die SMB-Serveroptionen, die auf der erweiterten Berechtigungsstufe verfügbar sind:

- **Erteilung von UNIX-Gruppenberechtigungen an CIFS-Server-Benutzer**

  Die Konfiguration dieser Option legt fest, ob einem CIFS-Benutzer, der nicht der Eigentümer der Datei ist, die Gruppenberechtigung erteilt werden kann. Wenn der CIFS-Benutzer nicht der Eigentümer der UNIX-Sicherheitsdatei ist und dieser Parameter auf `true` gesetzt ist, wird die Gruppenberechtigung für die Datei erteilt. Wenn der CIFS-Benutzer nicht der Eigentümer der UNIX-Sicherheitsdatei ist und dieser Parameter auf `false` gesetzt ist, gelten die normalen UNIX-Regeln für die Vergabe der Dateiberechtigung. Dieser Parameter ist für UNIX-Sicherheitsdateien mit der Berechtigung `mode bits` anwendbar und nicht für Dateien mit dem NTFS- oder NFSv4-Sicherheitsmodus. Die Standardeinstellung ist `false`.

- **Aktivieren oder Deaktivieren von SMB 1.0**

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

  > Ab ONTAP 9.3 ist SMB 1.0 für neue SMB Server standardmäßig deaktiviert. Zur Vorbereitung auf Sicherheits- und Compliance-Verbesserungen sollte so bald wie möglich auf eine neuere SMB Version migriert werden. Wenden Sie sich für Einzelheiten an Ihre NetApp Ansprechperson.

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

  SMB 2.0 ist die Mindestversion von SMB, die LIF-Failover unterstützt. Wenn SMB 2.x deaktiviert wird, deaktiviert ONTAP auch SMB 3.x automatisch.

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

- **Aktivieren oder Deaktivieren von SMB 3.0**

  SMB 3.0 ist die minimale SMB-Version, die dauerhaft verfügbare Freigaben unterstützt. Windows Server 2012 und Windows 8 sind die minimalen Windows-Versionen, die SMB 3.0 unterstützen.

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

- **Aktivieren oder Deaktivieren des ODX Copy Offloads**

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

- **Aktivieren oder Deaktivieren des Direktkopiermechanismus für ODX Copy Offload**

  Der Direktkopiermechanismus verbessert die Leistung des Copy-Offload-Vorgangs, 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 Direktkopiermechanismus aktiviert.

- **Automatische Knoten-Weiterleitungen aktivieren oder deaktivieren**

  Bei der automatischen Knotenweiterleitung verweist der SMB-Server Clients automatisch auf eine Daten-LIF, die lokal auf dem Knoten liegt, der die über die angeforderte Freigabe abgerufenen Daten hostet.

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

  Diese Option ist standardmäßig deaktiviert.

- **Aktivieren oder Deaktivieren der Verwendung von Verbindungspunkten als Reparse Points**

  Wenn diese Option aktiviert ist, stellt der SMB-Server Verbindungspunkte SMB-Clients als Reparse-Punkte zur Verfügung. 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 auf SVMs standardmäßig aktiviert.

- **Konfigurieren der maximalen Anzahl gleichzeitiger Operationen pro TCP-Verbindung**

  Der Standardwert ist 255.

- **Aktivieren oder Deaktivieren der lokalen Windows-Benutzer- und Gruppenfunktionalität**

  Diese Option ist standardmäßig aktiviert.

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

  Diese Option ist standardmäßig aktiviert.

- **Aktivieren oder Deaktivieren der VSS-Schattenkopiefunktionalität**

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

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

- **Konfiguration der Verzeichnistiefe des Schattenkopie-Verzeichnisses**

  Durch die Konfiguration dieser Option kann die maximale Verzeichnistiefe festgelegt werden, für die beim Verwenden der Schattenkopiefunktion Schattenkopien erstellt werden.

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

- **Aktivieren oder Deaktivieren der multidomain Suchfunktionen für die Namenszuordnung**

  Wenn diese Option aktiviert ist und ein UNIX-Benutzer mithilfe eines Platzhalters (*) im Domänenteil des Windows-Benutzernamens einem Windows-Domänenbenutzer zugeordnet wird (z. B. *\joe), sucht ONTAP nach dem angegebenen Benutzer in allen Domänen mit bidirektionalen Vertrauensstellungen zur Stammdomäne. Die Stammdomäne ist die Domäne, die das Computerkonto des SMB-Servers enthält.

  Alternativ zur Suche in allen bidirektional vertrauenswürdigen Domänen kann eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert werden. Wenn diese Option aktiviert ist und eine bevorzugte Liste konfiguriert wurde, wird die bevorzugte Liste für multidomain Namenszuordnungs-Suchen verwendet.

  Standardmäßig sind Suchen nach multidomain Namenszuordnungen aktiviert.

- **Konfigurieren der Sektorgröße des Dateisystems**

  Durch die Konfiguration dieser Option können Sie die Sektorgröße des Dateisystems in Bytes festlegen, die ONTAP an SMB-Clients meldet. Es gibt zwei gültige Werte: `4096` und `512`. Der Standardwert ist `4096`. Dieser Wert muss möglicherweise auf `512` gesetzt werden, wenn die Windows-Anwendung nur eine Sektorgröße von 512 Byte unterstützt.

- **Dynamische Zugriffskontrolle aktivieren oder deaktivieren**

  Durch Aktivieren dieser Option ist es möglich, Objekte auf dem SMB-Server mithilfe der Dynamic Access Control (DAC) zu schützen, einschließlich der Verwendung von Auditing zur Vorbereitung zentraler Zugriffsrichtlinien und der Verwendung von Group Policy Objects zur Implementierung zentraler Zugriffsrichtlinien. Die Option ist standardmäßig deaktiviert.

  Diese Option wird nur auf SVMs unterstützt.

- **Zugriffsbeschränkungen für nicht authentifizierte Sitzungen (anonyme Sitzungen einschränken)**

  Durch die Einstellung dieser Option werden die Zugriffsbeschränkungen für nicht authentifizierte Sitzungen festgelegt. Die Beschränkungen gelten für anonyme Benutzer. Standardmäßig gibt es keine Zugriffsbeschränkungen für anonyme Benutzer.

- **Aktivieren oder Deaktivieren der Darstellung von NTFS-ACLs auf Volumes mit effektiver UNIX-Sicherheit (UNIX-Sicherheitsstil-Volumes oder gemischte Sicherheitsstil-Volumes mit effektiver UNIX-Sicherheit)**

  Das Aktivieren oder Deaktivieren dieser Option bestimmt, wie die Dateisicherheit von Dateien und Ordnern mit UNIX-Sicherheit SMB-Clients präsentiert 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 Funktion**

  Durch Aktivierung dieser Funktion wird die Leistung von SMB 2.x und SMB 3.0 verbessert, indem die Art und Weise optimiert wird, wie ONTAP beim Abfragen von Attributinformationen für Dateien und Verzeichnisse Öffnungs- und Schließanforderungen stellt. Die SMB Fake Open Funktionalität ist standardmäßig aktiviert. Diese Option ist nur für Verbindungen mit SMB 2.x oder höher nützlich.

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

  Durch Aktivieren dieser Option werden UNIX-Erweiterungen auf einem SMB-Server aktiviert. UNIX-Erweiterungen ermöglichen die Anzeige von POSIX/UNIX-Sicherheit über das SMB-Protokoll. Standardmäßig ist diese Option deaktiviert.

  Wenn Sie in Ihrer Umgebung UNIX-basierte SMB-Clients wie Mac OSX Clients haben, empfiehlt sich die Aktivierung von UNIX-Erweiterungen. Die Aktivierung von UNIX-Erweiterungen ermöglicht es dem SMB-Server, POSIX/UNIX-Sicherheitsinformationen über SMB an den UNIX-basierten Client zu übertragen, der diese Informationen dann in POSIX/UNIX-Sicherheit übersetzt.

- **Aktivieren oder Deaktivieren der Unterstützung für Kurznamensuchen**

  Durch Aktivieren dieser Option kann der SMB-Server auch nach Kurznamen suchen. Eine Suchanfrage mit aktivierter Option versucht, sowohl 8.3-Dateinamen als auch lange Dateinamen zu finden. Der Standardwert für diesen Parameter ist `false`.

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

  Durch Aktivieren oder Deaktivieren dieser Option wird festgelegt, ob SMB-Server DFS-Funktionen automatisch gegenüber SMB 2.x- und SMB 3.0-Clients bekanntgeben, die eine Verbindung zu Freigaben herstellen. ONTAP verwendet DFS-Verweise bei der Implementierung von Symbol-Links für den SMB-Zugriff. Ist die Option aktiviert, gibt der SMB-Server die DFS-Funktionen immer bekannt, unabhängig davon, ob der Zugriff auf Symbol-Links aktiviert ist. Ist die Option deaktiviert, gibt der SMB-Server die DFS-Funktionen nur dann bekannt, wenn Clients eine Verbindung zu Freigaben herstellen, bei denen der Zugriff auf Symbol-Links aktiviert ist.

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

  Ab ONTAP 9.4 ermöglicht die Konfiguration der `-max-credits` Option, die Anzahl der Credits zu begrenzen, die auf einer SMB-Verbindung vergeben werden, wenn Clients und Server SMB Version 2 oder höher verwenden. Der Standardwert ist 128.

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

  Durch Aktivierung der `-is-multichannel-enabled` Option in ONTAP 9.4 und späteren Versionen kann der SMB-Server mehrere Verbindungen für eine einzelne SMB-Sitzung herstellen, wenn geeignete NICs im

Cluster und auf den Clients bereitgestellt sind. Dadurch werden Durchsatz und Fehlertoleranz verbessert. Der Standardwert für diesen Parameter ist `false`.

Wenn SMB Multichannel aktiviert ist, können auch die folgenden Parameter angegeben werden:

- 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.

## ONTAP SMB-Serveroptionen konfigurieren

Die SMB-Serveroptionen lassen sich jederzeit konfigurieren, nachdem ein SMB-Server auf einer Storage Virtual Machine (SVM) erstellt wurde.

**Schritt**

1. Die gewünschte Aktion ausführen:

| Wenn Sie Optionen für den SMB-Server konfigurieren möchten… | Geben Sie den Befehl ein… |
|---|---|
| Auf Administratorebene | `vserver cifs options modify -vserver` *`vserver_name options`* |
| Auf der Stufe „Erweiterte Berechtigungen“ | a. `set -privilege advanced`<br>b. `vserver cifs options modify -vserver` *`vserver_name options`*<br>c. `set -privilege admin` |

Weitere Informationen zu `vserver cifs options modify` und zur Konfiguration von SMB-Serveroptionen finden Sie in der "ONTAP-Befehlsreferenz".

## Die UNIX-Gruppenberechtigung für ONTAP SMB-Benutzer konfigurieren

Diese Option kann so konfiguriert werden, 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. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Die Berechtigung für die UNIX-Gruppe wird entsprechend konfiguriert:

| Wenn Sie möchten | Den Befehl eingeben |
|---|---|
| Der Zugriff auf Dateien oder Verzeichnisse ermöglicht das Erhalten von Gruppenberechtigungen, auch wenn der Benutzer nicht der Eigentümer der Datei ist. | `vserver cifs options modify –grant-unix-group-perms-to-others true` |

| Wenn Sie möchten | Den Befehl eingeben |
| --- | --- |
| Der Zugriff auf Dateien oder Verzeichnisse wird deaktiviert, sodass Gruppenberechtigungen nur dann gelten, wenn der Benutzer nicht der Eigentümer der Datei ist. | `vserver cifs options modify -grant-unix-group-perms-to-others false` |

3. Es wird überprüft, ob die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Zurück zur Administratorrechteebene: `set -privilege admin`

## ONTAP SMB-Zugriffsbeschränkungen für anonyme Benutzer konfigurieren

Standardmäßig kann ein anonymer, nicht authentifizierter Benutzer (auch als *null user* bezeichnet) auf bestimmte Informationen im Netzwerk zugreifen. Eine SMB-Serveroption ermöglicht die Konfiguration von Zugriffsbeschränkungen für den anonymen Benutzer.

### Über diese Aufgabe

Die `-restrict-anonymous`SMB Server Option entspricht dem `RestrictAnonymous`Registrierungseintrag in Windows.

Anonyme Benutzer können bestimmte Arten von Systeminformationen von Windows-Hosts im Netzwerk auflisten oder aufzählen, darunter Benutzernamen und Details, Kontorichtlinien und Freigabenamen. Der Zugriff für den anonymen Benutzer kann durch die Angabe einer von drei Zugriffsbeschränkungseinstellungen gesteuert werden:

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

### Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Die Einstellung „Anonyme Nutzer einschränken“ konfigurieren: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Es wird überprüft, ob die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver` *`vserver_name`*
4. Zurück zur Administratorrechteebene: `set -privilege admin`

### Verwandte Informationen

Verfügbare Serveroptionen

# Steuerung der Darstellung der Dateisicherheit für SMB-Clients bei UNIX-Sicherheitsstil-Daten

## Informationen zur Präsentation der ONTAP Dateisicherheit für SMB-Clients bei Daten im UNIX-Sicherheitsstil

Sie können festlegen, wie die Dateisicherheit für UNIX-Sicherheitsstil-Daten gegenüber SMB-Clients dargestellt wird, indem Sie die Anzeige von NTFS-ACLs für SMB-Clients aktivieren oder deaktivieren. Jede Einstellung bietet Vorteile, die verstanden werden sollten, um die am besten zu den Geschäftsanforderungen passende Einstellung auszuwählen.

Standardmäßig präsentiert ONTAP UNIX-Berechtigungen auf UNIX-Sicherheitsstil-Volumes SMB-Clients als NTFS-ACLs. Es gibt Szenarien, in denen dies wünschenswert ist, einschließlich der folgenden:

- UNIX-Berechtigungen lassen sich über die Registerkarte **Sicherheit** im Windows-Eigenschaftenfenster anzeigen und bearbeiten.

  Sie können Berechtigungen von einem Windows-Client aus nicht ändern, wenn der Vorgang vom UNIX-System nicht zugelassen wird. Beispielsweise können Sie den Besitz einer Datei, die Ihnen nicht gehört, nicht ändern, da das UNIX-System diesen Vorgang nicht erlaubt. Diese Einschränkung verhindert, dass SMB-Clients die auf Dateien und Ordnern festgelegten UNIX-Berechtigungen umgehen.

- Benutzer bearbeiten und speichern Dateien auf dem UNIX-Sicherheitsstil-Volume mithilfe bestimmter Windows-Anwendungen, zum Beispiel Microsoft Office, wobei ONTAP die UNIX-Berechtigungen während der Speichervorgänge beibehalten muss.
- Bestimmte Windows-Anwendungen in Ihrer Umgebung erwarten, NTFS-ACLs auf den von ihnen verwendeten Dateien lesen zu können.

Unter bestimmten Umständen kann es sinnvoll sein, die Darstellung von UNIX-Berechtigungen als NTFS-ACLs zu deaktivieren. Wenn diese Funktion deaktiviert ist, stellt ONTAP UNIX-Sicherheitsvolumes SMB-Clients als FAT-Volumes dar. Es gibt spezifische Gründe, warum UNIX-Sicherheitsvolumes SMB-Clients als FAT-Volumes präsentiert werden sollten:

- UNIX-Berechtigungen werden nur über Mounts auf UNIX-Clients geändert.

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

- Sie verwenden Anwendungen über SMB, die NTFS-ACLs für die aufgerufenen Dateien und Ordner festlegen, was fehlschlagen kann, wenn sich die Daten auf UNIX Security-Style-Volumes befinden.

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

**Verwandte Informationen**

- Sicherheitsstile auf FlexVol Volumes konfigurieren
- Sicherheitsstile für Qtrees konfigurieren

## Die Darstellung von NTFS-ACLs für ONTAP SMB-Clients bei UNIX-Sicherheitsstil-Daten konfigurieren

Die Anzeige von NTFS-ACLs für SMB-Clients bei Daten im UNIX-Sicherheitsstil (Volumes im UNIX-Sicherheitsstil und gemischte Volumes im Sicherheitsstil mit effektiver UNIX-Sicherheit) kann aktiviert oder deaktiviert werden.

**Über diese Aufgabe**

Wenn diese Option aktiviert ist, präsentiert ONTAP Dateien und Ordner auf Volumes mit effektivem UNIX-Sicherheitsstil für SMB-Clients als mit NTFS-ACLs versehen. Wenn diese Option deaktiviert ist, werden die Volumes SMB-Clients als FAT-Volumes präsentiert. Standardmäßig werden NTFS-ACLs für SMB-Clients präsentiert.

**Schritte**

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Konfiguration der UNIX NTFS ACL-Optionseinstellung: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Es wird überprüft, ob die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver` *`vserver_name`*
4. Zurück zur Administratorrechteebene: `set -privilege admin`

## Informationen zur Beibehaltung von UNIX-Berechtigungen für ONTAP SMB FlexVol Volumes

Wenn Dateien in einem FlexVol volume, die aktuell über UNIX-Berechtigungen verfügen, 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 Sicherheitseigenschaften der Datei, erstellen eine neue temporäre Datei, wenden diese Eigenschaften auf die temporäre Datei an und geben der temporären Datei dann den ursprünglichen Dateinamen.

Wenn Windows-Clients die Sicherheitseigenschaften abfragen, erhalten sie eine konstruierte ACL, die exakt den UNIX-Berechtigungen entspricht. Der einzige Zweck dieser konstruierten ACL besteht darin, die UNIX-Berechtigungen der Datei zu erhalten, wenn Dateien durch Windows-Anwendungen aktualisiert werden, sodass die resultierenden Dateien dieselben UNIX-Berechtigungen haben. ONTAP setzt mit der konstruierten ACL keine NTFS-ACLs.

## Informationen zur Verwaltung von UNIX-Berechtigungen über die Registerkarte „Windows-Sicherheit“ für ONTAP SMB-Server

Wenn UNIX-Berechtigungen von Dateien oder Ordnern in gemischten Security-Style-Volumes oder Qtrees auf SVMs bearbeitet werden sollen, steht die Registerkarte „Sicherheit“ auf Windows-Clients zur Verfügung. Alternativ können Anwendungen verwendet werden, die Windows-ACLs abfragen und festlegen.

- Ändern von UNIX-Berechtigungen

  Über die Registerkarte „Windows-Sicherheit“ können Sie UNIX-Berechtigungen für ein Volume oder einen

Qtree mit gemischtem Sicherheitsstil anzeigen und ändern. Wenn Sie die UNIX-Berechtigungen über die Hauptregisterkarte „Windows-Sicherheit“ ändern, muss zunächst die vorhandene ACE, die bearbeitet werden soll, entfernt werden (dadurch werden die Modusbits auf 0 gesetzt), bevor Änderungen vorgenommen werden. Alternativ kann der erweiterte Editor zum Ändern der Berechtigungen verwendet werden.

Wenn Modusberechtigungen verwendet werden, lassen sich die Modusberechtigungen für die angegebene UID, GID und andere (alle weiteren mit einem Konto auf dem Computer) direkt ändern. Wenn die angezeigte UID beispielsweise r-x-Berechtigungen hat, können die UID-Berechtigungen auf rwx geändert werden.

- UNIX-Berechtigungen in NTFS-Berechtigungen ändern

  Die Registerkarte „Windows-Sicherheit“ ermöglicht das Ersetzen von UNIX-Sicherheitsobjekten durch Windows-Sicherheitsobjekte auf einem Volume oder qtree mit gemischtem Sicherheitsstil, wenn die Dateien und Ordner einen effektiven UNIX-Sicherheitsstil aufweisen.

  Sie müssen zunächst alle aufgelisteten UNIX-Berechtigungseinträge entfernen, bevor Sie diese durch die gewünschten Windows User und Group Objekte ersetzen können. Anschließend können NTFS-basierte ACLs für die Windows User und Group Objekte konfiguriert werden. Durch das Entfernen aller UNIX-Sicherheitsobjekte und das Hinzufügen nur von Windows Usern und Groups zu einer Datei oder einem Ordner in einem Volume oder qtree mit gemischtem Sicherheitsstil ändert sich der effektive Sicherheitsstil der Datei oder des Ordners von UNIX zu NTFS.

  Wenn die Berechtigungen eines Ordners geändert werden, besteht das Standardverhalten von Windows darin, diese Änderungen auf alle Unterordner und Dateien zu übertragen. Daher muss die Auswahl zur Übertragung entsprechend angepasst werden, wenn eine Änderung des Sicherheitsstils nicht auf alle untergeordneten Ordner, Unterordner und Dateien übertragen werden soll.

# ONTAP SMB Multichannel für optimale Leistung und Redundanz konfigurieren

Ab ONTAP 9.4 kann SMB Multichannel so konfiguriert werden, dass mehrere Verbindungen zwischen ONTAP und Clients in einer einzigen SMB-Sitzung bereitgestellt werden. Dadurch werden Durchsatz und Fehlertoleranz verbessert.

**Bevor Sie beginnen**

Die SMB Multichannel-Funktionalität steht nur zur Verfügung, wenn Clients SMB 3.0 oder eine höhere Version aushandeln. SMB 3.0 und höher ist auf dem ONTAP SMB-Server standardmäßig aktiviert.

**Über diese Aufgabe**

SMB-Clients erkennen und nutzen automatisch mehrere Netzwerkverbindungen, wenn eine geeignete Konfiguration im ONTAP Cluster vorhanden ist.

Die Anzahl der gleichzeitigen Verbindungen in einer SMB-Sitzung hängt von den eingesetzten Netzwerkkarten (NICs) ab:

- **1G-NICs auf Client- und ONTAP-Cluster**

  Der Client stellt pro Netzwerkkarte eine Verbindung her und bindet die Sitzung an alle Verbindungen.

- **10G Netzwerkkarten und Netzwerkkarten mit größerer Kapazität auf Client- und ONTAP Cluster**

Der Client stellt bis zu vier Verbindungen pro Netzwerkkarte her und bindet die Sitzung an alle Verbindungen. Der Client kann Verbindungen über mehrere 10G Netzwerkkarten und Netzwerkkarten mit größerer Kapazität herstellen.

Sie können außerdem die folgenden Parameter ändern (erweiterte Berechtigung):

- `-max-connections-per-session`

  Die maximal zulässige Anzahl von Verbindungen pro Multichannel-Sitzung. Der Standardwert beträgt 32 Verbindungen.

  Wenn mehr Verbindungen als die Standardeinstellung aktiviert werden sollen, sind entsprechende Anpassungen an der Clientkonfiguration erforderlich, die ebenfalls standardmäßig 32 Verbindungen vorsieht.

- `-max-lifs-per-session`

  Die maximale Anzahl der pro Multichannel-Sitzung angekündigten Netzwerkschnittstellen. Der Standardwert beträgt 256 Netzwerkschnittstellen.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. SMB Multichannel auf dem SMB-Server aktivieren:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Es sollte überprüft werden, ob ONTAP SMB Multichannel-Sitzungen meldet:

```
vserver cifs session show
```

4. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

**Beispiel**

Das folgende Beispiel zeigt Informationen zu allen SMB-Sitzungen an und zeigt mehrere Verbindungen für eine einzelne Sitzung:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
```

```
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

Das folgende Beispiel zeigt detaillierte Informationen zu einer SMB-Sitzung mit der session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

# Standardzuordnung von Windows-Benutzern zu UNIX-Benutzern auf dem SMB-Server konfigurieren

## Standardmäßigen ONTAP SMB UNIX Benutzer konfigurieren

Sie können den Standard-UNIX-Benutzer konfigurieren, der verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn keine

einzelnen Benutzer zwischen UNIX und Windows zugeordnet werden sollen. Alternativ sollte der Standard-UNIX-Benutzer nicht konfiguriert werden, wenn die Authentifizierung nicht zugeordneter Benutzer fehlschlagen soll.

**Über diese Aufgabe**

Standardmäßig lautet der Name des Standard-UNIX-Benutzers „`pcuser`“, was bedeutet, dass die Benutzerzuordnung zum Standard-UNIX-Benutzer standardmäßig aktiviert ist. Ein anderer Name kann als Standard-UNIX-Benutzer angegeben werden. Der angegebene Name muss in den für die Storage Virtual Machine (SVM) konfigurierten Namensdienstdatenbanken vorhanden sein. Wenn diese Option auf eine leere Zeichenkette gesetzt ist, kann niemand als UNIX-Standardbenutzer auf den CIFS-Server zugreifen. Das bedeutet, dass jeder Benutzer ein Konto in der Passwortdatenbank haben muss, bevor auf den CIFS-Server zugegriffen werden kann.

Damit ein Benutzer eine Verbindung zum CIFS-Server mit dem Standard-UNIX-Benutzerkonto herstellen kann, müssen die folgenden Voraussetzungen erfüllt sein:

- Der Benutzer ist authentifiziert.
- Der Benutzer befindet sich in der lokalen Windows-Benutzerdatenbank des CIFS-Servers, in der Heimatdomäne des CIFS-Servers oder in einer vertrauenswürdigen Domäne (wenn die Suche nach multidomain Namenszuordnungen auf dem CIFS-Server aktiviert ist).
- Der Benutzername ist nicht explizit einer leeren Zeichenkette zugeordnet.

**Schritte**

1. Den Standard-UNIX-Benutzer konfigurieren:

| Wenn Sie möchten … | Geben Sie … ein |
|---|---|
| Der Standard-UNIX-Benutzer “pcuser” wird verwendet. | `vserver cifs options modify -default -unix-user pcuser` |
| Ein anderes UNIX-Benutzerkonto als Standardbenutzer verwenden | `vserver cifs options modify -default -unix-user` *`user_name`* |
| Standard-UNIX-Benutzer deaktivieren | `vserver cifs options modify -default -unix-user ""` |

```
vserver cifs options modify -default-unix-user pcuser
```

2. Es sollte überprüft werden, ob der Standard-UNIX-Benutzer korrekt konfiguriert ist: `vserver cifs options show -vserver` *`vserver_name`*

   Im folgenden Beispiel sind sowohl der Standard-UNIX-Benutzer als auch der Gast-UNIX-Benutzer auf SVM vs1 so konfiguriert, dass sie den UNIX-Benutzer “pcuser” verwenden:

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
```

```
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

## Den Gast-ONTAP SMB UNIX-Benutzer konfigurieren

Die Konfiguration der Option „Gast-UNIX-Benutzer“ bewirkt, dass Benutzer, die sich von nicht vertrauenswürdigen Domänen anmelden, diesem Gast-UNIX-Benutzer zugeordnet werden und eine Verbindung zum CIFS-Server herstellen können. Alternativ kann, wenn die Authentifizierung von Benutzern aus nicht vertrauenswürdigen Domänen fehlschlagen soll, der Gast-UNIX-Benutzer nicht konfiguriert werden. Standardmäßig ist es nicht erlaubt, dass Benutzer aus nicht vertrauenswürdigen Domänen eine Verbindung zum CIFS-Server herstellen (das Gast-UNIX-Konto ist nicht konfiguriert).

### Über diese Aufgabe

Bei der Konfiguration des Gast-UNIX-Kontos ist Folgendes zu beachten:

- Kann der CIFS-Server den Benutzer nicht gegenüber einem Domänencontroller der Home-Domain, einer vertrauenswürdigen Domain oder der lokalen Datenbank authentifizieren und ist diese Option aktiviert, betrachtet der CIFS-Server den Benutzer als Gastbenutzer und ordnet ihn dem angegebenen UNIX-Benutzer zu.
- Wenn diese Option auf eine leere Zeichenkette gesetzt ist, ist der Gast-UNIX-Benutzer deaktiviert.
- Es ist erforderlich, einen UNIX-Benutzer zu erstellen, der als Gast-UNIX-Benutzer in einer der Name-Service-Datenbanken der Storage Virtual Machine (SVM) verwendet wird.
- Ein als Gastbenutzer angemeldeter Benutzer ist automatisch Mitglied der Gruppe BUILTIN\guests auf dem CIFS-Server.
- Die Option „homedirs-public“ gilt nur für authentifizierte Benutzer. Ein als Gast angemeldeter Benutzer besitzt kein Home Directory und kann nicht auf die Home Directory-Pfade anderer Benutzer zugreifen.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Eingeben… |
|---|---|
| Den Gast-UNIX-Benutzer konfigurieren | `vserver cifs options modify -guest -unix-user` *unix_name* |
| Den Gast-UNIX-Benutzer deaktivieren | `vserver cifs options modify -guest -unix-user ""` |

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Es sollte überprüft werden, ob der Gast-UNIX-Benutzer korrekt konfiguriert ist: `vserver cifs options show -vserver` *vserver_name*

   Im folgenden Beispiel sind sowohl der Standard-UNIX-Benutzer als auch der Gast-UNIX-Benutzer auf SVM vs1 so konfiguriert, dass sie den UNIX-Benutzer “pcuser” verwenden:

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

## Administratorgruppen dem ONTAP SMB-Stamm zuordnen

Wenn Sie in Ihrer Umgebung ausschließlich CIFS-Clients verwenden und Ihre Storage Virtual Machine (SVM) als Multiprotokoll-Speichersystem eingerichtet wurde, benötigen Sie mindestens ein Windows-Konto mit Root-Berechtigung für den Zugriff auf Dateien auf der SVM, andernfalls ist die Verwaltung der SVM nicht möglich, da nicht ausreichende Benutzerrechte vorhanden sind.

### Über diese Aufgabe

Wenn Ihr Speichersystem ausschließlich mit NTFS konfiguriert ist, verfügt das `/etc`Verzeichnis über eine Dateizugriffskontrollliste (ACL), die es der Administratorgruppe ermöglicht, auf die ONTAP Konfigurationsdateien zuzugreifen.

### Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Die CIFS-Server-Option, die die Administratorengruppe der root-Berechtigung zuordnet, entsprechend konfigurieren:

| Wenn Sie möchten… | Dann… |
|---|---|
| Administratorgruppenmitglieder der Root-Gruppe zuordnen | `vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true`Alle Konten in der Administratorgruppe werden als root betrachtet, selbst wenn kein `/etc/usermap.cfg` Eintrag vorhanden ist, der die Konten root zuordnet. Wenn eine Datei mit einem Konto erstellt wird, das zur Administratorgruppe gehört, ist die Datei im Besitz von root, wenn sie von einem UNIX-Client aus angezeigt wird. |
| Deaktivieren der Zuordnung der Mitglieder der Administratorgruppe zu Root | `vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false`Konten in der Administratorgruppe werden nicht mehr root zugeordnet. Es kann nur noch ein einzelner Benutzer explizit root zugeordnet werden. |

3. Es wird überprüft, ob die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver vserver_name`
4. Zurück zur Administratorrechteebene: `set -privilege admin`

# Informationen darüber, welche Benutzertypen über ONTAP SMB-Sitzungen verbunden sind, anzeigen

Sie können Informationen darüber anzeigen, welche Benutzertypen über SMB-Sitzungen verbunden sind. Dies kann dabei helfen sicherzustellen, dass nur der jeweils geeignete Benutzertyp über SMB-Sitzungen auf der Storage Virtual Machine (SVM) verbunden ist.

**Über diese Aufgabe**

Folgende Benutzertypen können sich über SMB-Sitzungen verbinden:

- `local-user`

  Als lokaler CIFS-Benutzer authentifiziert

- `domain-user`

  Authentifiziert als Domänenbenutzer (entweder aus der Home-Domain des CIFS-Servers oder aus einer vertrauenswürdigen Domäne)

- `guest-user`

  Als Gastbenutzer authentifiziert

- `anonymous-user`

  Als anonymer oder Null-Benutzer authentifiziert

**Schritte**

1. Es wird ermittelt, welcher Benutzertyp über eine SMB-Sitzung verbunden ist: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

| Wenn Informationen zum Benutzertyp für bestehende Sitzungen angezeigt werden sollen… | Führen Sie den folgenden Befehl aus… |
|---|---|
| Für alle Sitzungen mit einem bestimmten Benutzertyp | `vserver cifs session show -vserver *vserver_name* -user-type {local-user |
| domain-user | guest-user |
| anonymous-user}` | Für einen bestimmten Benutzer |

**Beispiele**

Der folgende Befehl zeigt Sitzungsinformationen zum Benutzertyp für Sitzungen auf SVM vs1 an, die vom Benutzer "` iepubs\user1`" eingerichtet wurden:

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

# ONTAP Befehlsoptionen zur Begrenzung des übermäßigen Ressourcenverbrauchs von Windows Clients

Die Optionen des `vserver cifs options modify` Befehls ermöglichen die Steuerung des Ressourcenverbrauchs von Windows-Clients. Dies kann hilfreich sein, wenn einzelne Clients den normalen Ressourcenverbrauch überschreiten, beispielsweise bei einer ungewöhnlich hohen Anzahl geöffneter Dateien, Sitzungen oder Änderungsbenachrichtigungsanforderungen.

Die folgenden Optionen zum `vserver cifs options modify` Befehl wurden hinzugefügt, um den Ressourcenverbrauch von Windows-Clients zu steuern. Wird der Maximalwert einer dieser Optionen überschritten, wird die Anfrage abgelehnt und eine EMS-Meldung gesendet. Eine EMS-Warnmeldung wird auch gesendet, wenn 80 Prozent des konfigurierten Grenzwerts für diese Optionen erreicht sind.

- `-max-opens-same-file-per-tree`

  Maximale Anzahl von Öffnungen derselben Datei pro CIFS-Baum

- `-max-same-user-sessions-per-connection`

  Maximale Anzahl von Sitzungen, die vom selben Benutzer pro Verbindung geöffnet sind

- `-max-same-tree-connect-per-session`

  Maximale Anzahl von Baumverbindungen auf derselben Freigabe pro Sitzung

- `-max-watches-set-per-tree`

  Maximale Anzahl von Überwachungen (auch bekannt als *change notifies*), die pro Baum eingerichtet werden

Weitere Informationen zu `vserver cifs options modify` finden sich in der "ONTAP-Befehlsreferenz".

Ab ONTAP 9.4 können Server, auf denen die SMB-Version 2 oder höher ausgeführt wird, die Anzahl der ausstehenden Anforderungen (*SMB-Credits*) begrenzen, die der Client über eine SMB-Verbindung an den Server senden kann. Die Verwaltung von SMB-Credits wird vom Client initiiert und vom Server gesteuert.

Die maximale Anzahl ausstehender Anfragen, die auf einer SMB-Verbindung genehmigt werden können, wird durch die `-max-credits` Option gesteuert. Der Standardwert für diese Option ist 128.

# Die Client-Performance mit traditionellen und Lease-Oplocks verbessern

## Informationen zur Verbesserung der ONTAP SMB-Client-Performance mit traditionellen und Lease-Oplocks

Herkömmliche Oplocks (opportunistische Sperren) und Lease-Oplocks ermöglichen einem SMB-Client in bestimmten Dateifreigabeszenarien, Client-seitig Caching von Read-Ahead-, Write-Behind- und Sperrinformationen durchzuführen. Ein Client kann dann auf eine Datei lesend oder schreibend zugreifen, ohne den Server regelmäßig daran zu erinnern, dass er Zugriff auf die betreffende Datei benötigt. Dies verbessert die Leistung, da der Netzwerkverkehr reduziert wird.

Lease-Oplocks sind eine erweiterte Form von Oplocks, die ab dem SMB 2.1-Protokoll verfügbar sind. Lease-Oplocks ermöglichen es einem Client, den Client-Caching-Status über mehrere von ihm selbst initiierte SMB-Öffnungen hinweg zu erhalten und zu bewahren.

Oplocks können auf zwei Arten gesteuert werden:

- Durch eine Freigabeeigenschaft, mit dem `vserver cifs share create` Befehl beim Erstellen der Freigabe oder dem `vserver share properties` Befehl nach der Erstellung.
- Durch eine Qtree-Eigenschaft, mit dem `volume qtree create` Befehl beim Erstellen des Qtree oder den `volume qtree oplock` Befehlen nach der Erstellung.

## Informationen zu Überlegungen zum Datenverlust im ONTAP SMB-Cache beim Einsatz von Oplocks

Unter bestimmten Umständen muss ein Prozess, der eine exklusive Oplock-Sperre für eine Datei hält, wenn ein zweiter Prozess versucht, die Datei zu öffnen, zwischengespeicherte Daten ungültig machen und Schreibvorgänge sowie Sperren leeren. Der Client muss anschließend die Oplock-Sperre und den Zugriff auf die Datei freigeben. Tritt während dieses Leervorgangs ein Netzwerkausfall auf, können zwischengespeicherte Schreibdaten verloren gehen.

- Möglichkeiten für Datenverlust

  Jede Anwendung, die Daten im Schreibcache speichert, kann diese Daten unter den folgenden Umständen verlieren:

  - Die Verbindung wird über SMB 1.0 hergestellt.
  - Es verfügt über eine exklusive Oplock für die Datei.
  - Es wird angewiesen, entweder die Oplock Sperre aufzuheben oder die Datei zu schließen.
  - Beim Leeren des Schreibcaches erzeugt das Netzwerk oder das Zielsystem einen Fehler.
- Fehlerbehandlung und Schreibabschluss

  Der Cache selbst verfügt über keine Fehlerbehandlung, die Anwendungen übernehmen diese. Wenn die Anwendung einen Schreibvorgang in den Cache ausführt, wird der Schreibvorgang immer abgeschlossen. Wenn der Cache seinerseits einen Schreibvorgang über ein Netzwerk an das Zielsystem ausführt, muss er

davon ausgehen, dass der Schreibvorgang abgeschlossen ist, da die Daten andernfalls verloren gehen.

## Oplocks beim Erstellen von ONTAP SMB-Freigaben aktivieren oder deaktivieren

Oplocks ermöglichen es Clients, Dateien zu sperren und Inhalte lokal zwischenzuspeichern, was die Leistung bei Dateivorgängen verbessern kann. Oplocks sind für SMB-Freigaben auf Storage Virtual Machines (SVMs) aktiviert. In manchen Fällen kann es sinnvoll sein, Oplocks zu deaktivieren. Oplocks können für jede Freigabe einzeln aktiviert oder deaktiviert werden.

### Über diese Aufgabe

Wenn Oplocks auf dem Volume, das eine Freigabe enthält, aktiviert sind, die Oplock-Freigabeeigenschaft für diese Freigabe jedoch deaktiviert ist, sind Oplocks für diese Freigabe deaktiviert. Die Deaktivierung von Oplocks für eine Freigabe hat Vorrang vor der Oplock-Einstellung des Volumes. Durch die Deaktivierung von Oplocks für die Freigabe werden sowohl opportunistische als auch Lease-Oplocks deaktiviert.

Neben der Angabe der Oplock-Freigabeeigenschaft können auch weitere Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste angegeben werden. Es können auch andere Freigabeparameter angegeben werden.

### Schritte

1. Die entsprechende Maßnahme ausführen:

| Wenn Sie möchten… | Dann… |
| --- | --- |
| Oplocks bei der Freigabeerstellung aktivieren | Geben Sie den folgenden Befehl ein: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]`<br><br>Wenn die Freigabe nur die Standardeigenschaften `oplocks`, `browsable` und `changenotify` aktiviert haben soll, muss der `-share-properties` Parameter beim Erstellen einer SMB-Freigabe nicht angegeben werden. Wenn eine andere Kombination von Freigabeeigenschaften als die Standardwerte gewünscht ist, muss der `-share-properties` Parameter mit der Liste der zu verwendenden Freigabeeigenschaften für diese Freigabe angegeben werden. |

| Wenn Sie möchten… | Dann… |
| --- | --- |
| Oplocks während der Freigabeerstellung deaktivieren | Geben Sie den folgenden Befehl ein: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]`<br><br>Wenn Oplocks deaktiviert werden, muss beim Erstellen der Freigabe eine Liste von Freigabeeigenschaften angegeben werden, die `oplocks` Eigenschaft sollte jedoch nicht angegeben werden. |

**Verwandte Informationen**

Oplocks auf bestehenden SMB-Freigaben aktivieren oder deaktivieren

Oplock-Status überwachen

## ONTAP Befehle zum Aktivieren oder Deaktivieren von Oplocks auf SMB-Volumes und Qtrees

Oplocks ermöglichen es Clients, Dateien zu sperren und Inhalte lokal zwischenzuspeichern, was die Leistung bei Dateivorgängen verbessern kann. Sie müssen die Befehle zum Aktivieren oder Deaktivieren von Oplocks auf Volumes oder Qtrees kennen. Sie müssen außerdem wissen, wann Oplocks auf Volumes und Qtrees aktiviert oder deaktiviert werden können.

- Oplocks sind auf Volumes standardmäßig aktiviert.
- Oplocks können beim Erstellen eines Volumes nicht deaktiviert werden.
- Sie können Oplocks auf bestehenden Volumes für SVMs jederzeit aktivieren oder deaktivieren.
- Sie können Oplocks auf Qtrees für SVMs aktivieren.

  Die Oplock-Modus-Einstellung ist eine Eigenschaft des Qtree mit der ID 0, dem Standard-Qtree, den alle Volumes haben. Wird beim Erstellen eines Qtree keine Oplock-Einstellung angegeben, übernimmt der Qtree die Oplock-Einstellung des übergeordneten Volumes, die standardmäßig aktiviert ist. Wird jedoch eine Oplock-Einstellung für den neuen Qtree angegeben, hat diese Vorrang vor der Oplock-Einstellung des Volumes.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
| --- | --- |
| Oplocks auf Volumes oder Qtrees aktivieren | `volume qtree oplocks` mit dem `-oplock-mode` Parameter auf `enable` gesetzt |
| Oplocks auf Volumes oder Qtrees deaktivieren | `volume qtree oplocks` mit dem `-oplock-mode` Parameter auf `disable` gesetzt |

**Verwandte Informationen**

## Oplocks auf bestehenden ONTAP SMB-Freigaben aktivieren oder deaktivieren

Oplocks sind auf SMB-Freigaben auf Storage Virtual Machines (SVMs) standardmäßig aktiviert. Unter bestimmten Umständen kann es sinnvoll sein, Oplocks zu deaktivieren; alternativ kann, falls Oplocks zuvor für eine Freigabe deaktiviert wurden, eine erneute Aktivierung erfolgen.

### Über diese Aufgabe

Wenn Oplocks auf dem Volume, das eine Freigabe enthält, aktiviert sind, die Oplock-Freigabeeigenschaft für diese Freigabe jedoch deaktiviert ist, sind Oplocks für diese Freigabe deaktiviert. Die Deaktivierung von Oplocks für eine Freigabe hat Vorrang vor der Aktivierung von Oplocks für das Volume. Durch die Deaktivierung von Oplocks für die Freigabe werden sowohl opportunistische als auch Lease Oplocks deaktiviert. Oplocks können für bestehende Freigaben jederzeit aktiviert oder deaktiviert werden.

### Schritt

1. Die entsprechende Maßnahme ausführen:

| Wenn Sie möchten… | Dann… |
| --- | --- |
| Oplocks für eine Freigabe aktivieren, indem eine bestehende Freigabe geändert wird | Geben Sie den folgenden Befehl ein: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks`<br><br>Sie können zusätzliche Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste angeben.<br><br>Neu hinzugefügte Eigenschaften werden der bestehenden Liste der Share-Eigenschaften hinzugefügt. Alle zuvor festgelegten Share-Eigenschaften bleiben bestehen. |
| Oplocks für eine Freigabe durch Ändern einer bestehenden Freigabe deaktivieren | Geben Sie den folgenden Befehl ein: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks`<br><br>Sie können zusätzliche zu entfernende Freigabeeigenschaften mit einer durch Kommas getrennten Liste angeben.<br><br>Die von Ihnen entfernten Freigabeeigenschaften werden aus der bestehenden Liste der Freigabeeigenschaften gelöscht; zuvor konfigurierte Freigabeeigenschaften, die Sie nicht entfernen, bleiben jedoch weiterhin wirksam. |

#### Beispiele

Der folgende Befehl aktiviert Oplocks für die Freigabe mit dem Namen “Engineering” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

Der folgende Befehl deaktiviert Oplocks für die Freigabe mit dem Namen “Engineering” auf SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

#### Verwandte Informationen

- Oplocks beim Erstellen von SMB-Freigaben aktivieren oder deaktivieren
- Oplock-Status überwachen
- Freigabeeigenschaften bei bestehenden Shares hinzufügen oder entfernen

## ONTAP SMB Oplock-Status überwachen

Informationen zum Oplock-Status können überwacht und angezeigt werden. Diese Informationen ermöglichen die Feststellung, welche Dateien Oplocks haben, welches Oplock-Level und welcher Oplock-Status vorliegen und ob Oplock-Leasing verwendet wird. Es lässt sich außerdem ermitteln, welche Informationen zu Sperren vorliegen, die möglicherweise manuell aufgehoben werden müssen.

#### Über diese Aufgabe

Informationen zu allen Oplocks können in zusammengefasster oder detaillierter Listenform angezeigt werden. Optionale Parameter ermöglichen die Anzeige von Informationen zu einer kleineren Teilmenge der vorhandenen Sperren. So kann beispielsweise festgelegt werden, dass nur Sperren mit der angegebenen Client-IP-Adresse oder dem angegebenen Pfad ausgegeben werden.

Folgende Informationen über traditionelle und Lease-Oplocks können angezeigt werden:

- SVM, Knoten, Volume und LIF, auf denen der Oplock besteht
- Lock-UUID
- IP-Adresse des Clients mit dem Oplock
- Pfad, auf dem der Oplock etabliert wird
- Sperrprotokoll (SMB) und Typ (oplock)
- Sperrzustand
- Oplock-Ebene
- Verbindungsstatus und SMB-Ablaufzeit
- Open Group ID, wenn ein Lease Oplock gewährt wird

Weitere Informationen zu `vserver oplocks show` finden sich in der "ONTAP-Befehlsreferenz".

**Schritte**

1. Der Oplock-Status wird mit dem `vserver locks show` Befehl angezeigt.

**Beispiele**

Der folgende Befehl zeigt Standardinformationen zu allen Sperren an. Die Oplock-Sperre für die angezeigte Datei ist mit einer `read-batch` Oplock-Ebene vergeben:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

Das folgende Beispiel zeigt detailliertere Informationen zur Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Eine Lease Oplock wird für die Datei mit einem `batch` Oplock-Level an einen Client mit der IP-Adresse `10.3.1.3` gewährt:

Bei der Anzeige detaillierter Informationen liefert der Befehl separate Ausgaben für Oplock- und Sharelock-Informationen. Dieses Beispiel zeigt nur die Ausgabe des Oplock-Abschnitts.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
```

```
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

**Verwandte Informationen**

Oplocks beim Erstellen von SMB-Freigaben aktivieren oder deaktivieren

Oplocks auf bestehenden SMB-Freigaben aktivieren oder deaktivieren

Befehle zum Aktivieren oder Deaktivieren von Oplocks auf SMB-Volumes und Qtrees

# Gruppenrichtlinienobjekte auf SMB-Server anwenden

## Informationen zur Anwendung von Gruppenrichtlinienobjekten auf ONTAP SMB Servern

Ihr SMB-Server unterstützt Gruppenrichtlinienobjekte (GPOs), eine Reihe von Regeln, die als *Gruppenrichtlinienattribute* bezeichnet werden und für Computer in einer Active Directory-Umgebung gelten. Mit GPOs lassen sich die Einstellungen für alle Storage Virtual Machines (SVMs) im Cluster, die zur selben Active Directory-Domäne gehören, zentral verwalten.

Wenn Gruppenrichtlinienobjekte (GPOs) auf Ihrem SMB-Server aktiviert sind, sendet ONTAP LDAP-Abfragen an den Active Directory-Server, um GPO-Informationen anzufordern. Wenn GPO-Definitionen vorhanden sind, die für Ihren SMB-Server gelten, gibt der Active Directory-Server die folgenden GPO-Informationen zurück:

- GPO-Name
- Aktuelle GPO Version

- Speicherort der GPO-Definition
- Listen von UUIDs (universell eindeutigen Kennungen) für GPO Richtliniensätze

**Verwandte Informationen**

- Informationen zur Dateizugriffsicherheit für Server
- "SMB und NFS Auditierung und Sicherheitsverfolgung"

## Informationen zu unterstützten ONTAP SMB Gruppenrichtlinienobjekten

Obwohl nicht alle Gruppenrichtlinienobjekte (GPOs) auf Ihre CIFS-aktivierten Storage Virtual Machines (SVMs) anwendbar sind, können SVMs die relevanten GPOs erkennen und verarbeiten.

Die folgenden Gruppenrichtlinienobjekte (GPOs) werden derzeit auf SVMs unterstützt:

- Erweiterte Konfigurationseinstellungen für Überwachungsrichtlinien:

  Objektzugriff: Staging der zentralen Zugriffsrichtlinie

  Gibt die Art der Ereignisse an, die für das Staging der zentralen Zugriffsrichtlinie (CAP) geprüft werden, einschließlich der folgenden Einstellungen:

  - Keine Prüfung durchführen
  - Nur erfolgreiche Ereignisse prüfen
  - Nur Fehlerereignisse protokollieren
  - Sowohl Erfolgs- als auch Misserfolgsereignisse werden geprüft.

  > Wenn eine der drei Prüfoptionen ausgewählt ist (nur Erfolgsereignisse prüfen, nur Fehlerereignisse prüfen, sowohl Erfolgs- als auch Fehlerereignisse prüfen), prüft ONTAP sowohl Erfolgs- als auch Fehlerereignisse.

  Festgelegt durch die `Audit Central Access Policy Staging` Einstellung in der `Advanced Audit Policy Configuration/Audit Policies/Object Access` Gruppenrichtlinie.

  > Um die erweiterten Revisionsprotokoll-Gruppenrichtlinie-Konfigurationseinstellungen zu verwenden, muss die Überwachung auf der CIFS-Server-aktivierten SVM konfiguriert sein, auf die diese Einstellungen angewendet werden sollen. Wenn die Überwachung auf der SVM nicht konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und verworfen.

- Registrierungseinstellungen:

  - Gruppenrichtlinie Aktualisierungsintervall für CIFS-fähige SVMs

    Festgelegt durch die Verwendung der `Registry` Gruppenrichtlinie.

  - Gruppenrichtlinien-Aktualisierung zufälliger Offset

    Festgelegt durch die Verwendung der `Registry` Gruppenrichtlinie.

  - Hash-Veröffentlichung für BranchCache

Die Hash-Veröffentlichung für BranchCache GPO entspricht dem BranchCache Betriebsmodus. Die folgenden drei unterstützten Betriebsmodi werden unterstützt:

- Pro Aktie
- Alle Shares
- Deaktiviert, festgelegt durch die Verwendung der `Registry` Gruppenrichtlinie.

◦ Hash-Version-Unterstützung für BranchCache

Folgende drei Hash-Versionseinstellungen werden unterstützt:

- BranchCache Version 1
- BranchCache Version 2
- BranchCache Versionen 1 und 2 werden mithilfe der `Registry` Gruppenrichtlinie festgelegt.

> Um BranchCache GPO-Einstellungen zu verwenden, muss BranchCache auf dem CIFS-fähigen SVM konfiguriert sein, auf den diese Einstellungen angewendet werden sollen. Wenn BranchCache nicht auf dem SVM konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und verworfen.

- Sicherheitseinstellungen

◦ Audit-Richtlinie und Ereignisprotokoll

- Anmeldeüberwachungsereignisse

Legt die Art der zu prüfenden Anmeldeereignisse fest, einschließlich der folgenden Einstellungen:

- Keine Prüfung durchführen
- Nur erfolgreiche Ereignisse prüfen
- Prüfung von Fehlerereignissen
- Sowohl Erfolgs- als auch Fehlerereignisse werden durch die `Audit logon events` Einstellung in der `Local Policies/Audit Policy` Gruppenrichtlinie geprüft.

> Wenn eine der drei Prüfoptionen ausgewählt ist (nur Erfolgsereignisse prüfen, nur Fehlerereignisse prüfen, sowohl Erfolgs- als auch Fehlerereignisse prüfen), prüft ONTAP sowohl Erfolgs- als auch Fehlerereignisse.

- Objektzugriff prüfen

Gibt die Art des zu überwachenden Objektzugriffs an, einschließlich der folgenden Einstellungen:

- Keine Prüfung durchführen
- Nur erfolgreiche Ereignisse prüfen
- Prüfung von Fehlerereignissen
- Sowohl Erfolgs- als auch Fehlerereignisse werden durch die `Audit object access` Einstellung in der `Local Policies/Audit Policy` Gruppenrichtlinie geprüft.

> Wenn eine der drei Prüfoptionen ausgewählt ist (nur Erfolgsereignisse prüfen, nur Fehlerereignisse prüfen, sowohl Erfolgs- als auch Fehlerereignisse prüfen), prüft

ONTAP sowohl Erfolgs- als auch Fehlerereignisse.

- Protokollaufbewahrungsmethode

  Gibt die Methode zur Aufbewahrung des Revisionsprotokolls an, einschließlich der folgenden Einstellungen:

  - Das Ereignisprotokoll wird überschrieben, wenn die Größe der Protokolldatei die maximale Protokollgröße überschreitet
  - Das Ereignisprotokoll darf nicht überschrieben werden (Protokoll manuell löschen) Dies wird über die `Retention method for security log` Einstellung in der `Event Log` Gruppenrichtlinie festgelegt.

- Maximale Loggröße

  Gibt die maximale Größe des Revisionsprotokolls an.

  Festgelegt durch die `Maximum security log size` Einstellung in der `Event Log` Gruppenrichtlinie.

  Um Gruppenrichtlinien für Überwachungsrichtlinien und Ereignisprotokolle zu verwenden, muss die Überwachung auf der CIFS-aktivierten SVM konfiguriert sein, auf die diese Einstellungen angewendet werden sollen. Wenn die Überwachung auf der SVM nicht konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und verworfen.

◦ Dateisystemsicherheit

Gibt eine Liste von Dateien oder Verzeichnissen an, auf die die Dateisicherheit über eine Gruppenrichtlinie angewendet wird.

Festgelegt durch die Verwendung der `File System` Gruppenrichtlinie.

Der Volume-Pfad, für den die Gruppenrichtlinie für die Dateisystemsicherheit konfiguriert ist, muss innerhalb der SVM vorhanden sein.

◦ Kerberos Richtlinie

- Maximale Taktabweichung

  Gibt die maximale Toleranz in Minuten für Taktsynchronisierung an.

  Festgelegt durch die `Maximum tolerance for computer clock synchronization` Einstellung in der `Account Policies/Kerberos Policy` Gruppenrichtlinie.

- Maximales Ticketalter

  Legt die maximale Gültigkeitsdauer des Benutzertickets in Stunden fest.

  Festgelegt durch die `Maximum lifetime for user ticket` Einstellung in der `Account Policies/Kerberos Policy` Gruppenrichtlinie.

- Maximales Alter für die Ticketverlängerung

Legt die maximale Lebensdauer in Tagen für die Verlängerung von Benutzertickets fest.

Festgelegt durch die `Maximum lifetime for user ticket renewal` Einstellung in der `Account Policies/Kerberos Policy` Gruppenrichtlinie.

- Zuweisung von Benutzerrechten (Privilegienrechte)
  - Verantwortung übernehmen

    Gibt die Liste der Benutzer und Gruppen an, die das Recht haben, die Eigentümerschaft an einem beliebigen sicherungsfähigen Objekt zu übernehmen.

    Festgelegt durch die `Take ownership of files or other objects` Einstellung in der `Local Policies/User Rights Assignment` Gruppenrichtlinie.
  - Sicherheitsberechtigung

    Gibt die Liste der Benutzer und Gruppen an, die Überwachungsoptionen für Objektzugriff auf einzelne Ressourcen wie Dateien, Ordner und Active Directory Objekte festlegen können.

    Festgelegt durch die `Manage auditing and security log` Einstellung in der `Local Policies/User Rights Assignment` Gruppenrichtlinie.
  - Benachrichtigungsberechtigung ändern (Traversierungsüberprüfung umgehen)

    Gibt die Liste der Benutzer und Gruppen an, die Verzeichnisstrukturen durchlaufen können, auch wenn die Benutzer und Gruppen keine Berechtigungen für das durchlaufene Verzeichnis besitzen.

  Dieselbe Berechtigung ist erforderlich, damit Benutzer Benachrichtigungen über Änderungen an Dateien und Verzeichnissen erhalten. Festgelegt durch die `Bypass traverse checking` Einstellung in der `Local Policies/User Rights Assignment` Gruppenrichtlinie.
- Registrierungswerte
  - Einstellung „Signing erforderlich“

    Gibt an, ob die erforderliche SMB-Signierung aktiviert oder deaktiviert ist.

  Festgelegt durch die `Microsoft network server: Digitally sign communications (always)` Einstellung in der `Security Options` Gruppenrichtlinie.
- Anonymen Zugriff einschränken

  Legt fest, welche Einschränkungen für anonyme Benutzer gelten, und umfasst die folgenden drei Gruppenrichtlinieneinstellungen:
  - Keine Auflistung der Security Account Manager (SAM)-Konten:

    Diese Sicherheitseinstellung legt fest, welche zusätzlichen Berechtigungen für anonyme Verbindungen zum Computer erteilt werden. Diese Option wird als `no-enumeration` in ONTAP angezeigt, wenn sie aktiviert ist.

    Festgelegt durch die `Network access: Do not allow anonymous enumeration of SAM accounts` Einstellung in der `Local Policies/Security Options` Gruppenrichtlinie.

- Keine Aufzählung der SAM-Konten und Freigaben

  Diese Sicherheitseinstellung legt fest, ob die anonyme Auflistung von SAM-Konten und Freigaben zulässig ist. Diese Option wird als `no-enumeration` in ONTAP angezeigt, wenn sie aktiviert ist.

  Festgelegt durch die `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Einstellung in der `Local Policies/Security Options` Gruppenrichtlinie.

- Anonymer Zugriff auf Freigaben und Named Pipes einschränken

  Diese Sicherheitseinstellung beschränkt den anonymen Zugriff auf Freigaben und Pipes. Diese Option wird als `no-access` in ONTAP angezeigt, wenn sie aktiviert ist.

  Festgelegt durch die `Network access: Restrict anonymous access to Named Pipes and Shares` Einstellung in der `Local Policies/Security Options` Gruppenrichtlinie.

  Bei der Anzeige von Informationen zu definierten und angewendeten Gruppenrichtlinien liefert das `Resultant restriction for anonymous user` Ausgabefeld Informationen über die resultierende Einschränkung der drei Einstellungen für die Einschränkung von anonymen Gruppenrichtlinienobjekten. Die möglichen resultierenden Einschränkungen sind wie folgt:

° `no-access`

Dem anonymen Benutzer wird der Zugriff auf die angegebenen Freigaben und Named Pipes verweigert, und die Aufzählung von SAM-Konten und Freigaben ist nicht möglich. Diese Einschränkung ist zu beobachten, wenn die `Network access: Restrict anonymous access to Named Pipes and Shares`GPO aktiviert ist.

° `no-enumeration`

Der anonyme Benutzer hat Zugriff auf die angegebenen Freigaben und Named Pipes, kann aber keine SAM-Konten und Freigaben auflisten. Diese Einschränkung tritt ein, wenn beide folgenden Bedingungen erfüllt sind:

- Die `Network access: Restrict anonymous access to Named Pipes and Shares`Gruppenrichtlinie ist deaktiviert.
- Entweder die `Network access: Do not allow anonymous enumeration of SAM accounts` oder die `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs sind aktiviert.

° `no-restriction`

Der anonyme Benutzer hat vollen Zugriff und kann Enumerationen verwenden. Diese Einschränkung tritt ein, wenn beide folgenden Bedingungen erfüllt sind:

- Die `Network access: Restrict anonymous access to Named Pipes and Shares`Gruppenrichtlinie ist deaktiviert.
- Sowohl die `Network access: Do not allow anonymous enumeration of SAM accounts` und `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs sind deaktiviert.
  - Eingeschränkte Gruppen

Sie können eingeschränkte Gruppen konfigurieren, um die Mitgliedschaft von integrierten oder benutzerdefinierten Gruppen zentral zu verwalten. Wird eine eingeschränkte Gruppe über eine Gruppenrichtlinie angewendet, wird die Mitgliedschaft einer lokalen CIFS-Servergruppe automatisch so festgelegt, dass sie den in der angewendeten Gruppenrichtlinie definierten Mitgliedschaftslisteneinstellungen entspricht.

Festgelegt durch die Verwendung der `Restricted Groups` Gruppenrichtlinie.

- Zentrale Zugriffsrichtlinieneinstellungen

  Gibt eine Liste zentraler Zugriffsrichtlinien an. Zentrale Zugriffsrichtlinien und die zugehörigen zentralen Zugriffsrichtlinienregeln legen die Zugriffsberechtigungen für mehrere Dateien auf der SVM fest.

**Verwandte Informationen**

- GPO-Unterstützung auf Servern aktivieren oder deaktivieren
- Informationen zur Dateizugriffsicherheit für Server
- "SMB und NFS Auditierung und Sicherheitsverfolgung"
- Die Server-Sicherheitseinstellungen anpassen
- Informationen zur Verwendung von BranchCache zum Zwischenspeichern von freigegebenen Inhalten in einer Zweigstelle
- Informationen zur Verwendung von ONTAP Signaturen zur Verbesserung der Netzwerksicherheit
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung
- Zugriffsbeschränkungen für anonyme Benutzer konfigurieren

## ONTAP SMB-Server Anforderungen für Gruppenrichtlinienobjekte

Um Gruppenrichtlinienobjekte (GPOs) mit Ihrem SMB-Server verwenden zu können, muss Ihr System mehrere Voraussetzungen erfüllen.

- SMB muss auf dem Cluster lizenziert sein. Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.
- Ein SMB-Server muss konfiguriert und einer Windows Active Directory-Domäne hinzugefügt werden.
- Der SMB-Server-Adminstatus muss aktiviert sein.
- Gruppenrichtlinienobjekte (GPOs) müssen für die Windows Active Directory Abteilung (OU) konfiguriert und angewendet werden, die das SMB-Server-Computerobjekt enthält.
- Die GPO-Unterstützung muss auf dem SMB-Server aktiviert sein.

## GPO-Unterstützung auf ONTAP SMB-Servern aktivieren oder deaktivieren

Die Unterstützung für Gruppenrichtlinienobjekte (GPO) kann auf einem CIFS-Server aktiviert oder deaktiviert werden. Wenn die GPO-Unterstützung auf einem CIFS-Server aktiviert ist, werden die entsprechenden GPOs, die in der Gruppenrichtlinie definiert sind (der Richtlinie, die auf die Organisationseinheit (OU) angewendet wird, die das CIFS-Server-Computerobjekt enthält), auf den CIFS-Server angewendet.

**Über diese Aufgabe**

> Gruppenrichtlinienobjekte (GPOs) können auf CIFS-Servern im Arbeitsgruppenmodus nicht aktiviert werden.

**Schritte**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Geben Sie den Befehl ein… |
|---|---|
| Gruppenrichtlinienobjekte aktivieren | `vserver cifs group-policy modify -vserver vserver_name -status enabled` |
| Gruppenrichtlinien deaktivieren | `vserver cifs group-policy modify -vserver vserver_name -status disabled` |

2. Es sollte überprüft werden, ob die GPO-Unterstützung den gewünschten Status aufweist: `vserver cifs group-policy show -vserver +vserver_name_`

   Der Gruppenrichtlinienstatus für CIFS-Server im Arbeitsgruppenmodus wird als “disabled” angezeigt.

**Beispiel**

Das folgende Beispiel aktiviert die GPO-Unterstützung auf der Storage Virtual Machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

**Verwandte Informationen**

Informationen zu unterstützten Gruppenrichtlinienobjekten (GPOs)

Serveranforderungen für Gruppenrichtlinien

Informationen zum Aktualisieren von Gruppenrichtlinienobjekten (GPOs) auf SMB-Servern

Gruppenrichtlinieneinstellungen auf SMB-Servern manuell aktualisieren

Informationen zu GPO-Konfigurationen anzeigen

## Informationen zum Aktualisieren von Gruppenrichtlinienobjekten (GPOs) auf ONTAP SMB-Servern

Standardmäßig ruft ONTAP alle 90 Minuten Änderungen an Gruppenrichtlinienobjekten (GPOs) ab und wendet diese an. Sicherheitseinstellungen werden alle 16 Stunden aktualisiert. Wenn GPOs aktualisiert werden sollen, um neue GPO-Richtlinieneinstellungen anzuwenden, bevor ONTAP sie automatisch aktualisiert, kann eine manuelle Aktualisierung auf einem CIFS-Server mit einem ONTAP-Befehl ausgelöst werden.

- Standardmäßig werden alle Gruppenrichtlinienobjekte (GPOs) alle 90 Minuten überprüft und bei Bedarf aktualisiert.

  Dieses Intervall ist konfigurierbar und kann über die `Refresh interval` und `Random offset` Gruppenrichtlinieneinstellungen festgelegt werden.

  ONTAP fragt Active Directory nach Änderungen an Gruppenrichtlinienobjekten (GPOs) ab. Sind die in Active Directory gespeicherten GPO-Versionsnummern höher als die auf dem CIFS-Server, ruft ONTAP die neuen GPOs ab und wendet sie an. Stimmen die Versionsnummern überein, werden die GPOs auf dem CIFS-Server nicht aktualisiert.

- Die Gruppenrichtlinienobjekte (GPOs) für die Sicherheitseinstellungen werden alle 16 Stunden aktualisiert.

  ONTAP ruft die Gruppenrichtlinienobjekte (GPOs) für Sicherheitseinstellungen alle 16 Stunden ab und wendet sie an, unabhängig davon, ob sich diese GPOs geändert haben oder nicht.

  > Der Standardwert von 16 Stunden kann in der aktuellen ONTAP Version nicht geändert werden. Es handelt sich um eine Standardeinstellung des Windows Clients.

- Alle Gruppenrichtlinienobjekte (GPOs) können manuell mit einem ONTAP Befehl aktualisiert werden.

  Dieser Befehl simuliert den Windows `gpupdate.exe`/force`-Befehl.

**Verwandte Informationen**

Gruppenrichtlinieneinstellungen auf SMB-Servern manuell aktualisieren

## Manuelle Aktualisierung der GPO-Einstellungen auf ONTAP SMB Servern

Wenn Sie die Gruppenrichtlinienobjekt (GPO)-Einstellungen auf Ihrem CIFS-Server sofort aktualisieren möchten, können Sie die Einstellungen manuell aktualisieren. Es ist möglich, nur geänderte Einstellungen zu aktualisieren oder eine Aktualisierung für alle Einstellungen zu erzwingen, einschließlich der Einstellungen, die zuvor angewendet wurden, sich aber nicht geändert haben.

**Schritt**

1. Die entsprechende Maßnahme ausführen:

| Wenn Sie ein Update durchführen möchten… | Geben Sie den Befehl ein… |
|---|---|
| Geänderte Gruppenrichtlinieneinstellungen | `vserver cifs group-policy update -vserver vserver_name` |
| Alle GPO-Einstellungen | `vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true` |

**Verwandte Informationen**

Informationen zum Aktualisieren von Gruppenrichtlinienobjekten (GPOs) auf SMB-Servern

## Informationen zu ONTAP SMB GPO-Konfigurationen

Informationen über Gruppenrichtlinienobjekt (GPO)-Konfigurationen, die in Active Directory definiert sind, sowie über GPO-Konfigurationen, die auf den CIFS-Server angewendet werden, können angezeigt werden.

### Über diese Aufgabe

Es ist möglich, Informationen zu allen GPO-Konfigurationen anzuzeigen, die im Active Directory der Domäne definiert sind, zu der der CIFS-Server gehört, oder nur Informationen zu den GPO-Konfigurationen, die auf einen CIFS-Server angewendet wurden.

### Schritte

1. Informationen zu GPO-Konfigurationen werden durch eine der folgenden Aktionen angezeigt:

| Wenn Informationen zu allen Gruppenrichtlinienkonfigurationen angezeigt werden sollen… | Geben Sie den Befehl ein… |
|---|---|
| In Active Directory definiert | `vserver cifs group-policy show-defined -vserver vserver_name` |
| Angewendet auf eine CIFS-aktivierte Storage Virtual Machine (SVM) | `vserver cifs group-policy show-applied -vserver vserver_name` |

### Beispiel

Das folgende Beispiel zeigt die im Active Directory definierten GPO-Konfigurationen, zu denen die CIFS-fähige SVM mit dem Namen vs1 gehört:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
```

```
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
```

```
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Das folgende Beispiel zeigt die auf die CIFS-aktivierte SVM vs1 angewendeten GPO-Konfigurationen:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
```

```
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
```

```
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

**Verwandte Informationen**

GPO-Unterstützung auf Servern aktivieren oder deaktivieren

## Informationen zu ONTAP SMB eingeschränkten Gruppenrichtlinien (GPOs) anzeigen

Detaillierte Informationen über eingeschränkte Gruppen, die als Gruppenrichtlinienobjekte (GPOs) in Active Directory definiert sind und auf den CIFS-Server angewendet werden, können angezeigt werden.

**Über diese Aufgabe**

Standardmäßig werden folgende Informationen angezeigt:

- Name der Gruppenrichtlinie
- Gruppenrichtlinienversion
- Link

  Gibt die Ebene an, auf der die Gruppenrichtlinie konfiguriert ist. Mögliche Ausgabewerte sind die folgenden:

  - `Local`wenn die Gruppenrichtlinie in ONTAP konfiguriert ist
  - `Site`wenn die Gruppenrichtlinie auf Standortebene im Domänencontroller konfiguriert ist
  - `Domain`wenn die Gruppenrichtlinie auf Domänenebene im Domänencontroller konfiguriert ist
  - `OrganizationalUnit`wenn die Gruppenrichtlinie auf Abteilungsebene (OU) im Domänencontroller konfiguriert ist
  - `RSOP` für die resultierende Menge von Richtlinien, die aus allen auf verschiedenen Ebenen definierten Gruppenrichtlinien abgeleitet werden
- Name der eingeschränkten Gruppe

- Die Benutzer und Gruppen, die der eingeschränkten Gruppe angehören und die nicht der eingeschränkten Gruppe angehören
- Die Liste der Gruppen, zu denen die eingeschränkte Gruppe hinzugefügt wird

  Eine Gruppe kann Mitglied anderer Gruppen als der hier aufgeführten Gruppen sein.

**Schritt**

1. Informationen zu allen eingeschränkten Gruppenrichtlinienobjekten für Gruppen werden angezeigt, wenn eine der folgenden Aktionen durchgeführt wird:

| **Wenn Informationen zu allen eingeschränkten Gruppenrichtlinienobjekten (GPOs) angezeigt werden sollen…** | **Geben Sie den Befehl ein…** |
|---|---|
| In Active Directory definiert | `vserver cifs group-policy restricted-group show-defined -vserver vserver_name` |
| Angewendet auf einen CIFS-Server | `vserver cifs group-policy restricted-group show-applied -vserver vserver_name` |

**Beispiel**

Das folgende Beispiel zeigt Informationen über eingeschränkte Gruppenrichtlinienobjekte (GPOs), die in der Active Directory Domäne definiert sind, zu der die CIFS-Server-fähige SVM mit dem Namen vs1 gehört:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

Das folgende Beispiel zeigt Informationen über eingeschränkte Gruppenrichtlinienobjekte (GPOs) für eingeschränkte Gruppen, die auf die CIFS-aktivierte SVM vs1 angewendet wurden:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

**Verwandte Informationen**

Informationen zu GPO-Konfigurationen anzeigen

## Informationen zu den zentralen Zugriffsrichtlinien von ONTAP SMB anzeigen

Es lassen sich detaillierte Informationen zu den in Active Directory definierten zentralen Zugriffsrichtlinien anzeigen. Es lassen sich auch Informationen zu den zentralen Zugriffsrichtlinien anzeigen, die über Gruppenrichtlinienobjekte (GPOs) auf den CIFS-Server angewendet werden.

**Über diese Aufgabe**

Standardmäßig werden folgende Informationen angezeigt:

- SVM-Name
- Name der zentralen Zugriffsrichtlinie
- SID
- Beschreibung
- Erstellungszeit
- Änderungszeit
- Mitgliedsregeln

> CIFS-Server im Arbeitsgruppenmodus werden nicht angezeigt, da sie keine Gruppenrichtlinien (GPOs) unterstützen.

**Schritt**

1. Informationen zu zentralen Zugriffsrichtlinien werden durch eine der folgenden Aktionen angezeigt:

| Wenn Informationen zu allen zentralen Zugriffsrichtlinien angezeigt werden sollen… | Geben Sie den Befehl ein… |
|---|---|
| In Active Directory definiert | `vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name* |
| Angewendet auf einen CIFS-Server | `vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name* |

**Beispiel**

Das folgende Beispiel zeigt Informationen zu allen zentralen Zugriffsrichtlinien, die in Active Directory definiert sind:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Das folgende Beispiel zeigt Informationen zu allen zentralen Zugriffsrichtlinien, die auf die Storage Virtual Machines (SVMs) im Cluster angewendet sind:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                  SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
```

```
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                  S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

**Verwandte Informationen**

- Informationen zur Dateizugriffsicherheit für Server
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln

## Informationen zu den zentralen Zugriffsrichtlinienregeln von ONTAP SMB anzeigen

Es lassen sich detaillierte Informationen zu zentralen Zugriffsrichtlinienregeln anzeigen, die mit in Active Directory definierten zentralen Zugriffsrichtlinien verknüpft sind. Es lassen sich außerdem Informationen zu zentralen Zugriffsrichtlinienregeln anzeigen, die über zentrale Zugriffsrichtlinien-Gruppenrichtlinienobjekte (GPOs) auf den CIFS-Server angewendet werden.

**Über diese Aufgabe**

Sie können detaillierte Informationen zu definierten und angewendeten zentralen Zugriffsrichtlinienregeln anzeigen. Standardmäßig werden folgende Informationen angezeigt:

- Vserver Name
- Name der zentralen Zugriffsregel
- Beschreibung
- Erstellungszeit
- Änderungszeit
- Aktuelle Berechtigungen
- Vorgeschlagene Berechtigungen
- Zielressourcen

| Wenn Informationen zu allen zentralen Zugriffsrichtlinienregeln angezeigt werden sollen, die mit zentralen Zugriffsrichtlinien verknüpft sind… | Geben Sie den Befehl ein… |
|---|---|
| In Active Directory definiert | `vserver cifs group-policy central-access-rule show-defined -vserver vserver_name` |
| Angewendet auf einen CIFS-Server | `vserver cifs group-policy central-access-rule show-applied -vserver vserver_name` |

**Beispiel**

Das folgende Beispiel zeigt Informationen zu allen zentralen Zugriffsrichtlinienregeln, die mit in Active Directory definierten zentralen Zugriffsrichtlinien verknüpft sind:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Das folgende Beispiel zeigt Informationen zu allen zentralen Zugriffsrichtlinienregeln, die mit zentralen Zugriffsrichtlinien verknüpft sind, die auf Storage Virtual Machines (SVMs) im Cluster angewendet werden:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
```

```
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

**Verwandte Informationen**

- Informationen zur Dateizugriffsicherheit für Server
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen

# ONTAP Befehle zur Verwaltung von Passwörtern für SMB-Server-Computerkonten

Sie müssen die Befehle zum Ändern, Zurücksetzen und Deaktivieren von Passwörtern sowie zum Konfigurieren automatischer Aktualisierungszeitpläne kennen. Es besteht außerdem die Möglichkeit, einen Zeitplan auf dem SMB Server zu konfigurieren, damit dieser automatisch aktualisiert wird.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Das Domänenkontokennwort wird geändert, wenn ONTAP mit AD-Diensten synchronisiert ist. | `vserver cifs domain password change` |
| Das Domänenkontokennwort wird zurückgesetzt, wenn ONTAP nicht mit den AD-Diensten synchronisiert ist. | `vserver cifs domain password reset` |
| SMB-Server für automatische Änderungen von Computerkontokennwörtern konfigurieren | `vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true` |
| Automatische Änderung von Computerkontokennwörtern auf SMB-Servern deaktivieren | `vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false` |

Weitere Informationen zu `vserver cifs domain password` finden sich in der "ONTAP-Befehlsreferenz".

# Domänencontrollerverbindungen verwalten

## Informationen zu ONTAP SMB erkannten Servern

Informationen zu erkannten LDAP-Servern und Domänencontrollern auf Ihrem CIFS-Server können angezeigt werden.

**Schritt**

1. Um Informationen zu den gefundenen Servern anzuzeigen, den folgenden Befehl eingeben: `vserver cifs domain discovered-servers show`

**Beispiel**

Das folgende Beispiel zeigt die erkannten Server für SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

**Verwandte Informationen**

- Server zurücksetzen und neu erkennen
- Server stoppen oder starten

## ONTAP SMB-Server zurücksetzen und neu erkennen

Durch das Zurücksetzen und erneute Erkennen von Servern auf Ihrem CIFS-Server kann der CIFS-Server gespeicherte Informationen über LDAP-Server und Domänencontroller verwerfen. Nach dem Verwerfen der Serverinformationen ruft der CIFS-Server aktuelle Informationen über diese externen Server ab. Dies kann hilfreich sein, wenn die verbundenen Server nicht ordnungsgemäß reagieren.

**Schritte**

1. Geben Sie den folgenden Befehl ein: `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Informationen zu den neu erkannten Servern anzeigen: `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

**Beispiel**

Das folgende Beispiel setzt Server für Storage Virtual Machine (SVM, früher bekannt als Vserver) vs1 zurück und entdeckt sie erneut:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

**Verwandte Informationen**

- Informationen zu den erkannten Servern anzeigen
- Server stoppen oder starten

## Verwaltung der ONTAP SMB Domain Controller-Erkennung

Ab ONTAP 9.3 können Sie den Standardprozess zur Ermittlung von Domänencontrollern (DCs) anpassen. Dadurch kann die Ermittlung auf Ihren Standort oder auf einen Pool bevorzugter DCs beschränkt werden, was je nach Umgebung zu Leistungsverbesserungen führen kann.

**Über diese Aufgabe**

Standardmäßig ermittelt der dynamische Discovery-Prozess alle verfügbaren DCs, einschließlich aller bevorzugten DCs, aller DCs am lokalen Standort und aller Remote-DCs. Diese Konfiguration kann in bestimmten Umgebungen zu Latenz bei der Authentifizierung und beim Zugriff auf Freigaben führen. Wenn der Pool der zu verwendenden DCs bereits festgelegt wurde oder die Remote-DCs unzureichend oder nicht erreichbar sind, kann die Ermittlungsmethode geändert werden.

In ONTAP 9.3 und späteren Versionen ermöglicht der `discovery-mode` Parameter des `cifs domain discovered-servers` Befehls die Auswahl einer der folgenden Erkennungsoptionen:

- Alle Domänencontroller in der Domäne werden erkannt.
- Es werden nur DCs am lokalen Standort erkannt.

  Der `default-site`Parameter für den SMB-Server kann so definiert werden, dass dieser Modus mit LIFs verwendet wird, die in „Sites und Dienste“ keinem Standort zugeordnet sind. Ab ONTAP 9.13.1 kann der Standardstandort auch als Fallback verwendet werden, falls ONTAP keine Standortinformationen für eine vertrauenswürdige Domäne ermitteln kann.

- Es findet keine Servererkennung statt, die SMB Server-Konfiguration hängt ausschließlich von den bevorzugten DCs ab.

  Um diesen Modus zu verwenden, müssen zuerst die bevorzugten Domänencontroller für den SMB-Server definiert werden.

**Bevor Sie beginnen**

Sie müssen sich auf der erweiterten Berechtigungsstufe befinden.

**Schritt**

1. Geben Sie die gewünschte Erkennungsoption an: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

   Optionen für den `mode` Parameter:

   - `all`

     Alle verfügbaren DCs ermitteln (Standard).

   - `site`

     Die DC-Erkennung ist auf den eigenen Standort beschränkt.

   - `none`

     Es werden nur bevorzugte Domänencontroller verwendet, und eine Erkennung findet nicht statt.

## Bevorzugte ONTAP SMB-Domänencontroller hinzufügen

ONTAP erkennt Domänencontroller automatisch über DNS. Optional ist es möglich, einen oder mehrere Domänencontroller zur Liste der bevorzugten Domänencontroller für eine bestimmte Domäne hinzuzufügen.

### Über diese Aufgabe

Existiert für die angegebene Domäne bereits eine Liste bevorzugter Domänencontroller, wird die neue Liste mit der bestehenden Liste zusammengeführt.

### Schritt

1. Um die Liste der bevorzugten Domänencontroller zu erweitern, wird folgender Befehl eingegeben: `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, …+`

   `-vserver *vserver_name*`Gibt den Namen der Storage Virtual Machine (SVM) an.

   `-domain *domain_name*`Gibt den vollqualifizierten Active Directory-Namen der Domäne an, zu der die angegebenen Domänencontroller gehören.

   `-preferred-dc *IP_address*,…` gibt eine oder mehrere IP-Adressen der bevorzugten Domänencontroller als durch Kommas getrennte Liste in der Reihenfolge der Präferenz an.

### Beispiel

Der folgende Befehl fügt die Domänencontroller 172.17.102.25 und 172.17.102.24 der Liste der bevorzugten Domänencontroller hinzu, die der SMB-Server auf SVM vs1 zur Verwaltung des externen Zugriffs auf die Domäne cifs.lab.example.com verwendet.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

### Verwandte Informationen

Befehle zur Verwaltung bevorzugter Domänencontroller

### ONTAP Befehle zur Verwaltung bevorzugter SMB-Domänencontroller

Sie müssen die Befehle zum Hinzufügen, Anzeigen und Entfernen bevorzugter Domänencontroller kennen.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Bevorzugten Domänencontroller hinzufügen | `vserver cifs domain preferred-dc add` |
| Bevorzugte Domänencontroller anzeigen | `vserver cifs domain preferred-dc show` |
| Einen bevorzugten Domänencontroller entfernen | `vserver cifs domain preferred-dc remove` |

Weitere Informationen zu `vserver cifs domain preferred-dc` finden sich in der "ONTAP-Befehlsreferenz".

#### Verwandte Informationen

Bevorzugte Domänencontroller hinzufügen

### Verschlüsselte Verbindungen zu ONTAP SMB-Domänencontrollern aktivieren

Ab ONTAP 9.8 kann angegeben werden, dass Verbindungen zu Domänencontrollern verschlüsselt werden.

#### Über diese Aufgabe

ONTAP erfordert die Verschlüsselung der Kommunikation mit Domänencontrollern (DC), wenn die `-encryption-required-for-dc-connection` Option auf `true` gesetzt ist; standardmäßig ist `false` eingestellt. Wenn die Option gesetzt ist, wird für ONTAP DC-Verbindungen ausschließlich das SMB3-Protokoll verwendet, da Verschlüsselung nur von SMB3 unterstützt wird.

Wenn verschlüsselte DC-Kommunikation erforderlich ist, wird die `-smb2-enabled-for-dc-connections` Option ignoriert, da ONTAP ausschließlich SMB3-Verbindungen aushandelt. Unterstützt ein DC weder SMB3 noch Verschlüsselung, stellt ONTAP keine Verbindung zu ihm her.

#### Schritt

1. Verschlüsselte Kommunikation mit dem DC aktivieren: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

# Null-Sitzungen ermöglichen den Zugriff auf Speicher in Nicht-Kerberos-Umgebungen.

### ONTAP SMB-Nullsitzungen ermöglichen den Zugriff auf Speicher in Nicht-Kerberos-Umgebungen

Der Zugriff über eine Null-Sitzung ermöglicht Berechtigungen für Netzwerkressourcen wie Speichersystemdaten sowie für Client-seitige Dienste, die unter dem lokalen System ausgeführt werden. Eine Null-Sitzung tritt auf, wenn ein Clientprozess das Konto „system“ verwendet, um auf eine Netzwerkressource zuzugreifen. Die Konfiguration einer Null-Sitzung ist spezifisch für die Nicht-Kerberos Authentifizierung.

## Wie ONTAP SMB Speichersysteme Null-Session-Zugriff bereitstellen, wird erläutert.

Da Null-Session-Shares keine Authentifizierung erfordern, müssen die IP-Adressen von Clients, die Zugriff auf Null-Sessions benötigen, auf dem Speichersystem abgebildet sein.

Standardmäßig können nicht zugeordnete Null-Sitzungs-Clients auf bestimmte ONTAP-Systemdienste wie die Freigabeaufzählung zugreifen, jedoch ist ihnen der Zugriff auf Daten des Speichersystems untersagt.

> ONTAP unterstützt Windows RestrictAnonymous Registrierungseinstellungswerte mit der `-restrict-anonymous` Option. Dadurch lässt sich steuern, in welchem Umfang nicht zugeordnete Null-Benutzer Systemressourcen anzeigen oder darauf zugreifen können. Beispielsweise kann die Freigabeauflistung und der Zugriff auf die IPC$ Freigabe (die versteckte Named-Pipe-Freigabe) deaktiviert werden. Weitere Informationen zu `vserver cifs options modify` und `vserver cifs options show` sowie zur `-restrict-anonymous` Option sind in der "ONTAP-Befehlsreferenz" zu finden.

Sofern nicht anders konfiguriert, ist ein Client, der einen lokalen Prozess ausführt, der über eine Null-Sitzung Zugriff auf das Storage-System anfordert, nur Mitglied von nicht einschränkenden Gruppen wie „`everyone`“. Um den Zugriff über Null-Sitzungen auf ausgewählte Storage-Systemressourcen zu beschränken, können Sie eine Gruppe erstellen, der alle Null-Sitzungs-Clients angehören. Die Erstellung dieser Gruppe ermöglicht es Ihnen, den Zugriff auf das Storage-System einzuschränken und Berechtigungen für Storage-Systemressourcen festzulegen, die speziell für Null-Sitzungs-Clients gelten.

ONTAP bietet eine Zuordnungssyntax im `vserver name-mapping`-Befehlssatz, um die IP-Adresse von Clients anzugeben, denen der Zugriff auf Speichersystemressourcen über eine Nullbenutzersitzung erlaubt ist. Nachdem eine Gruppe für Nullbenutzer erstellt wurde, lassen sich Zugriffsbeschränkungen für Speichersystemressourcen und Ressourcenberechtigungen festlegen, die ausschließlich für Nullsitzungen gelten. Ein Nullbenutzer wird als anonymer Logon identifiziert. Nullbenutzer haben keinen Zugriff auf ein Home-Verzeichnis.

Jedem Null-Benutzer, der von einer zugeordneten IP-Adresse auf das Speichersystem zugreift, werden die Berechtigungen des zugeordneten Benutzers gewährt. Es sind geeignete Vorkehrungen zu treffen, um unbefugten Zugriff auf Speichersysteme zu verhindern, die mit Null-Benutzern zugeordnet sind. Für maximalen Schutz empfiehlt es sich, das Speichersystem und alle Clients, die Zugriff als Null-Benutzer auf das Speichersystem benötigen, in einem separaten Netzwerk zu platzieren, um die Möglichkeit von IP-Adress-„Spoofing“ auszuschließen.

**Verwandte Informationen**

Zugriffsbeschränkungen für anonyme Benutzer konfigurieren

## Null-Benutzern Zugriff auf ONTAP SMB-Dateisystemfreigaben gewähren

Sie können Null-Session-Clients den Zugriff auf Ihre Speichersystemressourcen ermöglichen, indem Sie eine Gruppe zuweisen, die von Null-Session-Clients verwendet wird, und die IP-Adressen der Null-Session-Clients aufzeichnen, um sie der Liste der Clients des Speichersystems hinzuzufügen, die mit Null-Sessions auf Daten zugreifen dürfen.

**Schritte**

1. Mit dem `vserver name-mapping create`Befehl lässt sich der Null-Benutzer einem beliebigen gültigen Windows-Benutzer mit einem IP-Qualifizierer zuordnen.

Der folgende Befehl ordnet den Null-Benutzer dem Benutzer user1 mit dem gültigen Hostnamen google.com zu:

```
vserver name-mapping create -direction win-unix  -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

Der folgende Befehl ordnet den Null-Benutzer dem Benutzer user1 mit der gültigen IP-Adresse 10.238.2.54/32 zu:

```
vserver name-mapping create -direction win-unix  -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Mit dem `vserver name-mapping show` Befehl lässt sich die Namenszuordnung bestätigen.

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1       -                 10.72.40.83/32      Pattern: anonymous logon
                                           Replacement: user1
```

3. Mit dem `vserver cifs options modify –win-name-for-null-user` Befehl wird dem Benutzer „null“ die Windows-Mitgliedschaft zugewiesen.

   Diese Option ist nur anwendbar, wenn eine gültige Namenszuordnung für den Null-Benutzer vorhanden ist.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Mit dem `vserver cifs options show` Befehl lässt sich die Zuordnung des Null-Benutzers zum Windows-Benutzer oder zur Windows-Gruppe bestätigen.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

# NetBIOS-Aliase für SMB Server verwalten

## Informationen zur Verwaltung von NetBIOS-Aliasen für ONTAP SMB-Server

NetBIOS-Aliase sind alternative Namen für Ihren SMB-Server, die SMB-Clients beim Verbindungsaufbau mit dem SMB-Server verwenden können. Die Konfiguration von NetBIOS-Aliasen für einen SMB-Server kann nützlich sein, wenn Daten von anderen Dateiservern auf den SMB-Server zusammengeführt werden und der SMB-Server auf die Namen der ursprünglichen Dateiserver reagieren soll.

Sie können beim Erstellen des SMB-Servers oder jederzeit danach eine Liste von NetBIOS-Aliasen festlegen. NetBIOS-Aliase können jederzeit zur Liste hinzugefügt oder daraus entfernt werden. Eine Verbindung zum SMB-Server ist mit jedem der Namen in der NetBIOS-Aliasliste möglich.

**Verwandte Informationen**

Informationen zu NetBIOS over TCP-Verbindungen

## NetBIOS-Aliaslisten zu ONTAP SMB-Servern hinzufügen

Wenn SMB-Clients sich über einen Alias mit dem SMB-Server verbinden sollen, kann eine Liste von NetBIOS-Aliasen erstellt oder NetBIOS-Aliase zu einer bestehenden Liste von NetBIOS-Aliasen hinzugefügt werden.

**Über diese Aufgabe**

- Der NetBIOS-Aliasname darf maximal 15 Zeichen lang sein.
- Auf dem SMB-Server können bis zu 200 NetBIOS-Aliase konfiguriert werden.
- Folgende Zeichen sind nicht zulässig:

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

**Schritte**

1. Die NetBIOS-Aliase hinzufügen:
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - Sie können einen oder mehrere NetBIOS-Aliase mithilfe einer durch Kommas getrennten Liste angeben.
   - Die angegebenen NetBIOS-Aliase werden der bestehenden Liste hinzugefügt.
   - Eine neue Liste von NetBIOS-Aliasen wird erstellt, wenn die Liste derzeit leer ist.
2. Es sollte überprüft werden, ob die NetBIOS-Aliase korrekt hinzugefügt wurden: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

   ```
   Vserver: vs1

            Server Name: CIFS_SERVER
   ```

```
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

**Verwandte Informationen**

- NetBIOS-Aliase aus der Liste für SMB-Server entfernen
- NetBIOS-Aliasliste für SMB-Server

## NetBIOS-Aliase aus der Liste für ONTAP SMB-Server entfernen

Wenn keine bestimmten NetBIOS-Aliase für einen CIFS-Server benötigt werden, können diese NetBIOS-Aliase aus der Liste entfernt werden. Es ist auch möglich, alle NetBIOS-Aliase aus der Liste zu entfernen.

**Über diese Aufgabe**

Sie können mehr als einen NetBIOS-Alias mithilfe einer durch Kommas getrennten Liste entfernen. Alle NetBIOS-Aliase auf einem CIFS-Server können entfernt werden, indem - als Wert für den `-netbios-aliases` Parameter angegeben wird.

**Schritte**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie entfernen möchten… | Eingeben… |
|---|---|
| Spezifische NetBIOS Aliase aus der Liste | `vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios-aliases _NetBIOS_alias_,...` |
| Alle NetBIOS Aliase aus der Liste | `vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -` |

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Es wird überprüft, ob die angegebenen NetBIOS-Aliase entfernt wurden: `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_2, ALIAS_3
```

## NetBIOS-Aliasliste für ONTAP SMB-Server

Sie können die Liste der NetBIOS-Aliase anzeigen. Dies ist hilfreich, wenn die Liste der Namen ermittelt werden soll, über die SMB-Clients Verbindungen zum CIFS-Server herstellen können.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Informationen über … angezeigt werden sollen | Eingeben… |
|---|---|
| NetBIOS-Aliase eines CIFS-Servers | `vserver cifs show -display-netbios -aliases` |
| Die Liste der NetBIOS-Aliase als Teil der detaillierten CIFS-Server-Informationen | `vserver cifs show -instance` |

Das folgende Beispiel zeigt Informationen über die NetBIOS-Aliase eines CIFS-Servers:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Das folgende Beispiel zeigt die Liste der NetBIOS-Aliase als Teil der detaillierten CIFS-Server-Informationen:

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                      CIFS Server NetBIOS Name: CIFS_SERVER
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Weitere Informationen zu `vserver cifs show` finden sich in der "ONTAP-Befehlsreferenz".

**Verwandte Informationen**

- NetBIOS-Aliaslisten zu Servern hinzufügen
- Befehle zur Serververwaltung

## Feststellen, ob ONTAP SMB-Clients über NetBIOS-Aliase verbunden sind

Sie können feststellen, ob SMB-Clients über NetBIOS-Aliase verbunden sind und, falls ja, welcher NetBIOS-Alias für die Verbindung verwendet wird. Dies kann bei der Behebung

von Verbindungsproblemen hilfreich sein.

**Über diese Aufgabe**

Sie müssen den `-instance` Parameter verwenden, um den NetBIOS-Alias (falls vorhanden) anzuzeigen, der mit einer SMB-Verbindung verknüpft ist. Wenn für die SMB-Verbindung der CIFS-Servername oder eine IP-Adresse verwendet wird, ist die Ausgabe für das `NetBIOS Name` Feld – (Bindestrich).

**Schritt**

1. Die gewünschte Aktion ausführen:

| Wenn Sie NetBIOS-Informationen für … anzeigen möchten | Eingeben… |
|---|---|
| SMB-Verbindungen | `vserver cifs session show -instance` |
| Verbindungen mit einem angegebenen NetBIOS-Alias: | `vserver cifs session show -instance -netbios-name` *`netbios_name`* |

Das folgende Beispiel zeigt Informationen über den NetBIOS-Alias, der für die SMB-Verbindung mit der Sitzungs-ID 1 verwendet wird:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                  Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

# Verschiedene SMB Serveraufgaben verwalten

## ONTAP SMB-Server stoppen oder starten

Sie können den CIFS-Server auf einer SVM stoppen, was nützlich ist, wenn Aufgaben ausgeführt werden, während Benutzer nicht über SMB-Freigaben auf Daten zugreifen. Der SMB-Zugriff kann durch Starten des CIFS-Servers wiederhergestellt werden. Durch das Stoppen des CIFS-Servers können auch die auf der Storage Virtual Machine (SVM) zulässigen Protokolle geändert werden.

**Schritte**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Geben Sie den Befehl ein… |
|---|---|
| Den CIFS-Server anhalten | `vserver cifs stop -vserver *vserver_name* [-foreground {true |
| false}]` | CIFS-Server starten |
| `vserver cifs start -vserver *vserver_name* [-foreground {true | false}]` |

`-foreground` Gibt an, ob der Befehl im Vordergrund oder im Hintergrund ausgeführt wird. Wird dieser Parameter nicht eingegeben, ist er auf `true` gesetzt und der Befehl wird im Vordergrund ausgeführt.

2. Es kann mithilfe des `vserver cifs show` Befehls überprüft werden, ob der administrative Status des CIFS-Servers korrekt ist.

**Beispiel**

Die folgenden Befehle starten den CIFS-Server auf SVM vs1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                        Vserver: vs1
                      CIFS Server NetBIOS Name: VS1
                  NetBIOS Domain/Workgroup Name: DOMAIN
                    Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

**Verwandte Informationen**

- Informationen zu den erkannten Servern anzeigen
- Server zurücksetzen und neu erkennen

## ONTAP SMB-Server in andere Organisationseinheiten verschieben

Der CIFS-Server-Erstellungsprozess verwendet während der Einrichtung die Standard-

Organisationseinheit (OU) CN=Computers, sofern keine andere OU angegeben wird. CIFS-Server können nach der Einrichtung in andere OUs verschoben werden.

**Schritte**

1. Auf dem Windows-Server wird die Struktur **Active Directory Users and Computers** geöffnet.
2. Das Active Directory-Objekt für die Storage Virtual Machine (SVM) ermitteln.
3. Mit der rechten Maustaste auf das Objekt klicken und **Verschieben** auswählen.
4. Die Organisationseinheit, die mit der SVM verknüpft werden soll, auswählen.

**Ergebnisse**

Das SVM-Objekt befindet sich in der ausgewählten Organisationseinheit.

## Die dynamische DNS-Domäne vor dem Verschieben von ONTAP SMB-Servern anpassen.

Wenn der in Active Directory integrierte DNS-Server die DNS-Einträge des SMB-Servers dynamisch im DNS registrieren soll, wenn der SMB-Server in eine andere Domäne verschoben wird, muss dynamisches DNS (DDNS) auf der Storage Virtual Machine (SVM) vor dem Verschieben des SMB-Servers geändert werden.

**Bevor Sie beginnen**

Die DNS-Namensdienste auf der SVM müssen so angepasst werden, dass sie die DNS-Domäne verwenden, die die Service-Location-Einträge für die neue Domäne enthält, in der das SMB-Server-Computerkonto enthalten sein wird. Wenn sicheres DDNS verwendet wird, sind Active Directory-integrierte DNS-Namensserver erforderlich.

**Über diese Aufgabe**

Obwohl DDNS (sofern auf der SVM konfiguriert) die DNS-Einträge für Daten-LIFs automatisch zur neuen Domäne hinzufügt, werden die DNS-Einträge der ursprünglichen Domäne nicht automatisch vom ursprünglichen DNS-Server gelöscht. Diese müssen manuell gelöscht werden.

Um die DDNS-Änderungen vor dem Verschieben des SMB-Servers abzuschließen, siehe das folgende Thema:

"Dynamische DNS-Dienste konfigurieren"

## ONTAP SMB SVMs mit Active Directory-Domänen verbinden

Sie können eine Storage Virtual Machine (SVM) einer Active Directory-Domäne hinzufügen, ohne den vorhandenen SMB-Server zu löschen, indem Sie die Domäne mit dem `vserver cifs modify` Befehl ändern. Es besteht die Möglichkeit, der aktuellen Domäne erneut beizutreten oder einer neuen Domäne beizutreten.

**Bevor Sie beginnen**

- Die SVM muss bereits über eine DNS-Konfiguration verfügen.
- Die DNS-Konfiguration für die SVM muss die Zieldomäne bedienen können.

  Die DNS-Server müssen die Service Location Records (SRV) für die Domain LDAP und Domain Controller Server enthalten.

Beim Beitritt zu einer Active Directory-Domäne ohne vorheriges Löschen des vorhandenen SMB-Servers können verbleibende Kontoattribute oder eine unvollständige Initialisierung, wie z. B. die SID, der SPN oder die Vertrauensstellung, dazu führen, dass der Domänenname im Fenster **Location** nicht angezeigt wird.

Tritt dieses Problem auf, ist der vorhandene SMB-Server aus der Active Directory-Domäne zu entfernen und anschließend der Domäne erneut hinzuzufügen.

**Über diese Aufgabe**

- Der administrative Status des CIFS-Server muss auf `down` gesetzt werden, damit die Active Directory-Domäne geändert werden kann.
- Wenn der Befehl erfolgreich abgeschlossen wird, wird der administrative Status automatisch auf `up` gesetzt.
- Beim Beitritt zu einer Domäne kann die Ausführung dieses Befehls mehrere Minuten dauern.

**Schritte**

1. Die SVM wird mit der CIFS-Server-Domäne verbunden: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Weitere Informationen zu `vserver cifs modify` finden sich in der "ONTAP-Befehlsreferenz". Falls eine Neukonfiguration von DNS für die neue Domain erforderlich ist, stehen weitere Informationen zu `vserver dns modify` im "ONTAP-Befehlsreferenz" zur Verfügung.

   Um ein Active Directory Computerkonto für den SMB-Server zu erstellen, müssen der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen angegeben werden, um Computer zum `ou=` *`example`* `ou` Container innerhalb der *`example`*.com-Domäne hinzuzufügen.

   Ab ONTAP 9.7 kann Ihnen Ihr AD-Administrator als Alternative zu einem Namen und Passwort für ein privilegiertes Windows-Konto eine URI zu einer Keytab-Datei bereitstellen. Nach Erhalt der URI ist diese im `-keytab-uri` Parameter mit den `vserver cifs` Befehlen anzugeben.

2. Es sollte sichergestellt sein, dass sich der CIFS-Server in der gewünschten Active Directory-Domäne befindet: `vserver cifs show`

**Beispiel**

Im folgenden Beispiel tritt der SMB-Server “CIFSSERVER1” auf SVM vs1 der Domäne example.com mithilfe der Keytab-Authentifizierung bei:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

## Informationen zu ONTAP SMB NetBIOS über TCP-Verbindungen

Sie können Informationen zu NetBIOS over TCP (NBT)-Verbindungen anzeigen. Dies kann bei der Fehlerbehebung von NetBIOS-bezogenen Problemen hilfreich sein.

**Schritt**

1. Mit dem `vserver cifs nbtstat` Befehl werden Informationen zu NetBIOS over TCP-Verbindungen angezeigt.

   Der NetBIOS Name Service (NBNS) über IPv6 wird nicht unterstützt.

**Beispiel**

Das folgende Beispiel zeigt die NetBIOS-Namensdienstinformationen, die für “cluster1” angezeigt werden:

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
        Servers:
                   17.17.1.2  (active  )
        NBT Scope:
                  [ ]
        NBT Mode:
                  [h]
        NBT Name    NetBIOS Suffix   State   Time Left   Type
        ----------- ---------------  ------- ---------   -----
        CLUSTER_1   00               wins    57
        CLUSTER_1   20               wins    57

        Vserver: vs1
        Node:    cluster1-02
        Interfaces:
                10.10.10.35
        Servers:
                17.17.1.2  (active  )
        CLUSTER_1          00               wins          58
        CLUSTER_1          20               wins          58
        4 entries were displayed.
```

## ONTAP Befehle zur Verwaltung von SMB Servern

Sie müssen die Befehle zum Erstellen, Anzeigen, Ändern, Stoppen, Starten und Löschen von SMB Servern kennen. Es gibt außerdem Befehle zum Zurücksetzen und erneuten

Erkennen von Servern, zum Ändern oder Zurücksetzen von Maschinenkontopasswörtern, zum Planen von Änderungen für Maschinenkontopasswörter sowie zum Hinzufügen oder Entfernen von NetBIOS Aliassen.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Einen SMB Server erstellen | `vserver cifs create` |
| Informationen zu einem SMB Server anzeigen | `vserver cifs show` |
| Einen SMB Server modifizieren | `vserver cifs modify` |
| Verschieben eines SMB Servers in eine andere Domäne | `vserver cifs modify` |
| Anhalten eines SMB-Servers | `vserver cifs stop` |
| Einen SMB Server starten | `vserver cifs start` |
| Einen SMB Server löschen | `vserver cifs delete` |
| Server für den SMB Server zurücksetzen und neu erkennen | `vserver cifs domain discovered-servers reset-servers` |
| Das Kennwort des Maschinenkontos des SMB-Servers ändern | `vserver cifs domain password change` |
| Das Maschinenkontopasswort des SMB-Servers zurücksetzen | `vserver cifs domain password change` |
| Automatische Kennwortänderungen für das Computerkonto des SMB-Servers planen | `vserver cifs domain password schedule modify` |
| NetBIOS Aliase für den SMB Server hinzufügen | `vserver cifs add-netbios-aliases` |
| NetBIOS-Aliase für den SMB-Server entfernen | `vserver cifs remove-netbios-aliases` |

Weitere Informationen zu `vserver cifs` finden sich in der "ONTAP-Befehlsreferenz".

**Verwandte Informationen**

"Was mit lokalen Benutzern und Gruppen beim Löschen von SMB Servern geschieht"

## Den ONTAP SMB NetBios-Namensdienst aktivieren

Ab ONTAP 9 ist der NetBios-Namensdienst (NBNS, manchmal auch Windows Internet Name Service oder WINS genannt) standardmäßig deaktiviert. Früher sendeten CIFS-Server Storage Virtual Machines (SVMs) Namensregistrierungs-Broadcasts, unabhängig davon, ob WINS im Netzwerk aktiviert war. Um solche Broadcasts auf Konfigurationen zu beschränken, in denen NBNS erforderlich ist, muss NBNS für neue CIFS-Server explizit aktiviert werden.

**Bevor Sie beginnen**

- Wenn Sie bereits NBNS nutzen und auf ONTAP 9 aktualisieren, ist es nicht notwendig, diese Aufgabe durchzuführen. NBNS funktioniert weiterhin wie zuvor.
- NBNS ist über UDP (Port 137) aktiviert.

- NBNS über IPv6 wird nicht unterstützt.

**Schritte**

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt.

```
set -privilege advanced
```

2. NBNS auf einem CIFS-Server aktivieren.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Zurück zur Administrator-Berechtigungsstufe.

```
set -privilege admin
```

# IPv6 für SMB-Zugriff und SMB-Dienste verwenden

## Informationen zu den ONTAP SMB-Anforderungen für IPv6

Bevor Sie IPv6 auf Ihrem SMB-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB dies unterstützen und welche Lizenzanforderungen gelten.

### ONTAP Lizenzanforderungen

Für IPv6 ist keine spezielle Lizenz erforderlich, wenn SMB lizenziert ist. Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

### Anforderungen an die SMB-Protokollversion

- Für SVMs unterstützt ONTAP IPv6 auf allen Versionen des SMB-Protokolls.

Der NetBIOS Name Service (NBNS) über IPv6 wird nicht unterstützt.

## Informationen zur Unterstützung von IPv6 mit ONTAP SMB-Zugriff und CIFS-Services

Wenn Sie IPv6 auf Ihrem CIFS-Server verwenden möchten, ist es wichtig zu wissen, wie ONTAP IPv6 für den SMB-Zugriff und die Netzwerkkommunikation für CIFS-Dienste unterstützt.

### Windows Client- und Serverunterstützung

ONTAP bietet Unterstützung für Windows Server und Clients, die IPv6 unterstützen. Im Folgenden wird die IPv6-Unterstützung für Microsoft Windows Clients und Server beschrieben:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 und spätere Versionen unterstützen IPv6 sowohl für SMB-Dateifreigabe als auch für Active Directory-Dienste, einschließlich DNS, LDAP, CLDAP und Kerberos-Dienste.

  Sind IPv6-Adressen konfiguriert, verwenden Windows 7 und Windows Server 2008 sowie spätere Versionen IPv6 standardmäßig für Active Directory Services. Sowohl NTLM- als auch Kerberos-Authentifizierung über IPv6-Verbindungen wird unterstützt.

  Alle von ONTAP unterstützten Windows-Clients können über IPv6-Adressen eine Verbindung zu SMB-Freigaben herstellen.

Die aktuellsten Informationen darüber, welche Windows-Clients ONTAP unterstützt, sind unter "Interoperabilitätsmatrix" zu finden.

NT-Domänen werden für IPv6 nicht unterstützt.

### Zusätzliche CIFS-Services-Unterstützung

Zusätzlich zur IPv6-Unterstützung für SMB-Dateifreigaben und Active Directory-Dienste bietet ONTAP IPv6-Unterstützung für Folgendes:

- Clientseitige Dienste, einschließlich Offline-Ordner, Roaming-Profile, Ordnerumleitung und Previous Versions
- Serverseitige Dienste, einschließlich dynamischer Home-Verzeichnisse (Home Directory-Funktion), Symlinks und Widelinks, BranchCache, ODX Copy Offload, automatische Node-Referrals und Previous Versions
- Dateizugriffsverwaltungsdienste, einschließlich der Verwendung von lokalen Windows-Benutzern und -Gruppen für Zugriffskontrolle und Rechteverwaltung, der Festlegung von Dateiberechtigungen und Überwachungsrichtlinien mit der CLI, Sicherheitsverfolgung, Verwaltung von Dateisperren und Überwachung der SMB-Aktivität
- NAS Multiprotokoll-Auditierung
- FPolicy
- Kontinuierlich verfügbare Freigaben, Witness-Protokoll und Remote VSS (verwendet mit Hyper-V über SMB Konfigurationen)

### Unterstützung für Namensdienste und Authentifizierungsdienste

Die Kommunikation mit den folgenden Namensdiensten wird mit IPv6 unterstützt:

- Domänencontroller
- DNS-Server
- LDAP-Server
- KDC-Server
- NIS-Server

## Es wird erläutert, wie ONTAP SMB-Server IPv6 verwenden, um eine Verbindung zu externen Servern herzustellen.

Um eine Konfiguration zu erstellen, die Ihren Anforderungen entspricht, ist es erforderlich, zu wissen, wie CIFS-Server IPv6 verwenden, wenn sie Verbindungen zu externen Servern herstellen.

- Auswahl der Quelladresse

  Wenn eine Verbindung zu einem externen Server hergestellt wird, muss die ausgewählte Quelladresse vom gleichen Typ wie die Zieladresse sein. Wenn beispielsweise eine Verbindung zu einer IPv6-Adresse hergestellt wird, muss die Storage Virtual Machine (SVM), auf der der CIFS-Server gehostet wird, über eine Daten-LIF oder eine Management-LIF mit einer IPv6-Adresse verfügen, die als Quelladresse verwendet werden kann. Entsprechend muss die SVM, wenn eine Verbindung zu einer IPv4-Adresse hergestellt wird, über eine Daten-LIF oder eine Management-LIF mit einer IPv4-Adresse verfügen, die als Quelladresse verwendet werden kann.

- Bei Servern, die dynamisch über DNS ermittelt werden, erfolgt die Serverermittlung wie folgt:
  - Wenn IPv6 auf dem Cluster deaktiviert ist, werden nur IPv4-Serveradressen ermittelt.
  - Wenn IPv6 im Cluster aktiviert ist, werden sowohl IPv4- als auch IPv6-Serveradressen ermittelt. Je nach Eignung des Servers, zu dem die Adresse gehört, und der Verfügbarkeit von IPv6- oder IPv4-Daten- oder Management-LIFs kann entweder der eine oder der andere Typ verwendet werden. Die dynamische Serverermittlung wird zur Erkennung von Domain Controllern und deren zugehörigen Diensten wie LSA, NETLOGON, Kerberos und LDAP verwendet.
- DNS Server-Konnektivität

  Ob die SVM beim Verbinden mit einem DNS-Server IPv6 verwendet, hängt von der Konfiguration der DNS-Namensdienste ab. Wenn die DNS-Dienste so konfiguriert sind, dass sie IPv6-Adressen verwenden, werden Verbindungen über IPv6 hergestellt. Falls gewünscht, kann die Konfiguration der DNS-Namensdienste IPv4-Adressen verwenden, sodass Verbindungen zu DNS-Servern weiterhin über IPv4-Adressen erfolgen. Bei der Konfiguration der DNS-Namensdienste können Kombinationen aus IPv4- und IPv6-Adressen angegeben werden.

- LDAP Server-Konnektivität

  Ob die SVM IPv6 für die Verbindung zu einem LDAP-Server verwendet, hängt von der LDAP-Client-Konfiguration ab. Wenn der LDAP-Client so konfiguriert ist, dass IPv6-Adressen verwendet werden, erfolgen die Verbindungen über IPv6. Falls gewünscht, kann die LDAP-Client-Konfiguration IPv4-Adressen verwenden, sodass Verbindungen zu LDAP-Servern weiterhin über IPv4-Adressen erfolgen. Bei der Konfiguration der LDAP-Client-Konfiguration können Kombinationen aus IPv4- und IPv6-Adressen angegeben werden.

  > Die LDAP-Client-Konfiguration wird verwendet, wenn LDAP für UNIX-Benutzer-, Gruppen- und Netzgruppennamendienste konfiguriert wird.

- NIS Server-Konnektivität

  Ob die SVM beim Verbinden mit einem NIS-Server IPv6 verwendet, hängt von der Konfiguration der NIS-Namensdienste ab. Wenn die NIS-Dienste so konfiguriert sind, dass sie IPv6-Adressen verwenden, werden Verbindungen über IPv6 hergestellt. Falls gewünscht, kann die Konfiguration der NIS-Namensdienste IPv4-Adressen verwenden, sodass Verbindungen zu NIS-Servern weiterhin über IPv4-Adressen erfolgen. Bei der Konfiguration der NIS-Namensdienste können Kombinationen aus IPv4- und

IPv6-Adressen angegeben werden.

> NIS-Namensdienste werden zum Speichern und Verwalten von UNIX-Benutzer-, Gruppen-, Netzgruppen- und Hostnamensobjekten verwendet.

**Verwandte Informationen**

- IPv6 für Server aktivieren
- Informationen zu IPv6-Sitzungen überwachen und anzeigen

## IPv6 für ONTAP SMB Server aktivieren

IPv6-Netzwerke sind während der Cluster-Einrichtung nicht aktiviert. Ein Cluster-Administrator muss IPv6 nach Abschluss der Cluster-Einrichtung aktivieren, um IPv6 für SMB zu verwenden. Wenn der Cluster-Administrator IPv6 aktiviert, ist es für den gesamten Cluster aktiviert.

**Schritt**

1. IPv6 aktivieren: `network options ipv6 modify -enabled true`

   IPv6 ist aktiviert. IPv6-Daten-LIFs für SMB-Zugriff können konfiguriert werden.

**Verwandte Informationen**

- Informationen zu IPv6-Sitzungen überwachen und anzeigen
- "Das Netzwerk mithilfe von System Manager visualisieren"
- "Aktivierung von IPv6 auf dem Cluster"
- "Netzwerkoptionen IPv6 ändern"

## Informationen zum Deaktivieren von IPv6 für ONTAP SMB Server

Auch wenn IPv6 im Cluster über eine Netzwerkoption aktiviert ist, kann IPv6 für SMB nicht mit demselben Befehl deaktiviert werden. Stattdessen deaktiviert ONTAP IPv6, wenn der Clusteradministrator die letzte IPv6-fähige Schnittstelle im Cluster deaktiviert. Eine Abstimmung mit dem Clusteradministrator zur Verwaltung der IPv6-fähigen Schnittstellen ist empfehlenswert.

**Verwandte Informationen**

- "Das ONTAP Netzwerk lässt sich mit System Manager visualisieren."

## Überwachung und Anzeige von Informationen zu IPv6 ONTAP SMB-Sitzungen

Sie können Informationen über SMB-Sitzungen überwachen und anzeigen, die über IPv6-Netzwerke verbunden sind. Diese Informationen sind hilfreich, um festzustellen, welche Clients sich über IPv6 verbinden, sowie weitere nützliche Informationen über IPv6 SMB-Sitzungen.

**Schritt**

1. Die gewünschte Aktion ausführen:

| Wenn Sie feststellen möchten, ob… | Geben Sie den Befehl ein… |
| --- | --- |
| SMB-Sitzungen zu einer Storage Virtual Machine (SVM) sind über IPv6 verbunden | `vserver cifs session show -vserver vserver_name -instance` |
| IPv6 wird für SMB-Sitzungen über eine bestimmte LIF-Adresse verwendet | `vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance`<br><br>*LIF_IP_address* ist die IPv6-Adresse des Daten-LIF. |

**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.