SMB mit der Befehlszeile verwalten

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/index.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

SMB mit der Befehlszeile verwalten . . . 1
Informationen zu ONTAP SMB . . . 1
SMB Server-Unterstützung . . . 1
Informationen zur Unterstützung von ONTAP SMB-Servern . . . 1
Unterstützte ONTAP SMB Versionen und Funktionen . . . 1
Nicht unterstützte Windows-Funktionen in ONTAP SMB . . . 3
NIS- oder LDAP-Namensdienste auf ONTAP SMB SVMs konfigurieren . . . 3
Informationen zur Konfiguration des ONTAP SMB Name Service Switch . . . 6
SMB Server verwalten . . . 8
ONTAP SMB-Server modifizieren . . . 8
Optionen zur Anpassung von SMB-Servern verwenden . . . 9
Steuerung der Darstellung der Dateisicherheit für SMB-Clients bei UNIX-Sicherheitsstil-Daten . . . 16
ONTAP SMB Multichannel für optimale Leistung und Redundanz konfigurieren . . . 18
Standardzuordnung von Windows-Benutzern zu UNIX-Benutzern auf dem SMB-Server konfigurieren . . . 20
Informationen darüber, welche Benutzertypen über ONTAP SMB-Sitzungen verbunden sind, anzeigen . . . 24
ONTAP Befehlsoptionen zur Begrenzung des übermäßigen Ressourcenverbrauchs von Windows Clients . . . 25
Die Client-Performance mit traditionellen und Lease-Oplocks verbessern . . . 25
Gruppenrichtlinienobjekte auf SMB-Server anwenden . . . 32
ONTAP Befehle zur Verwaltung von Passwörtern für SMB-Server-Computerkonten . . . 50
Domänencontrollerverbindungen verwalten . . . 51
Null-Sitzungen ermöglichen den Zugriff auf Speicher in Nicht-Kerberos-Umgebungen. . . . 55
NetBIOS-Aliase für SMB Server verwalten . . . 57
Verschiedene SMB Serveraufgaben verwalten . . . 61
IPv6 für SMB-Zugriff und SMB-Dienste verwenden . . . 66
SMB Server-Sicherheitseinstellungen verwalten . . . 70
Informationen zur Handhabung der ONTAP SMB Client-Authentifizierung . . . 70
Informationen zu den SMB-Server-Sicherheitseinstellungen für die ONTAP SVM-Disaster Recovery Konfiguration . . . 71
Informationen zu den Sicherheitseinstellungen des ONTAP SMB-Servers anzeigen . . . 71
ONTAP Passwortkomplexität für lokale SMB-Benutzer konfigurieren . . . 72
Die Kerberos-Sicherheitseinstellungen des ONTAP SMB-Servers ändern . . . 73
Das minimale Sicherheit bei der Authentifizierung Niveau des ONTAP SMB-Servers festlegen . . . 75
Starke ONTAP SMB-Sicherheit für Kerberos-basierte Kommunikation mit AES-Verschlüsselung konfigurieren . . . 76
AES-Verschlüsselung für die Kerberos-basierte Kommunikation von ONTAP SMB konfigurieren . . . 77
SMB-Signierung zur Erhöhung der Netzwerksicherheit verwenden . . . 80
Erforderliche SMB-Verschlüsselung auf SMB-Servern für Datenübertragungen über SMB konfigurieren . . . 90
Sichere LDAP-Sitzungskommunikation . . . 99
Dateizugriff mit SMB einrichten . . . 102
Sicherheitsstile konfigurieren . . . 102
Daten-Volumes in NAS-Namespaces erstellen und verwalten . . . 106

Namenszuordnungen konfigurieren . . . 111
Konfiguration von Namenszuordnungssuchen über mehrere Domänen hinweg . . . 116
SMB-Freigaben erstellen und konfigurieren . . . 121
Sicherer Dateizugriff mithilfe von SMB-Freigabe-ACLs . . . 130
Dateizugriff mithilfe von Dateiberechtigungen absichern . . . 134
Sicherer Dateizugriff durch Dynamic Access Control (DAC) . . . 138
SMB-Zugriff mithilfe von Exportrichtlinien absichern . . . 148
Sicherer Dateizugriff mit Storage Level Access Guard . . . 154
Dateizugriff mit SMB verwalten . . . 168
Lokale Benutzer und Gruppen für Authentifizierung und Autorisierung verwenden . . . 168
Umgehungsüberprüfung konfigurieren . . . 192
Informationen zu Dateisicherheit und Überwachungsrichtlinien . . . 195
NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf SVMs mithilfe der CLI verwalten . . . 213
Dateisicherheit für NTFS-Dateien und Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden . . . 218
Überwachungsrichtlinien für NTFS-Dateien und -Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden . . . 227
Informationen zur Verwaltung von ONTAP SMB-Sicherheitsrichtlinienjobs . . . 234
ONTAP Befehle zur Verwaltung von NTFS- und SMB-Sicherheitsrichtlinien und Zugriffskontrolleinträgen . . . 235
Den Metadatencache für SMB-Freigaben konfigurieren . . . 237
Dateisperren verwalten . . . 239
SMB-Aktivitäten überwachen . . . 244
SMB-Client-basierte Dienste bereitstellen . . . 253
Offline-Dateien ermöglichen das Zwischenspeichern von Dateien für die Offline-Nutzung. . . . 254
Roaming-Profile dienen dazu, Benutzerprofile zentral auf einem mit der SVM verbundenen SMB-Server zu speichern. . . . 259
Die Ordnerumleitung ermöglicht das Speichern von Daten auf einem SMB-Server. . . . 261
Informationen zum Zugriff auf das ONTAP ~snapshot-Verzeichnis von Windows-Clients mit SMB 2.x . . . 262
Dateien und Ordner mit vorherigen Versionen wiederherstellen . . . 263
Bereitstellung von SMB serverbasierten Diensten . . . 268
Home-Verzeichnisse verwalten . . . 268
Konfiguration des SMB-Client-Zugriffs auf UNIX Symbol-Links . . . 281
Erfahren Sie mehr über BranchCache . . . 289
Konfiguration von BranchCache auf ONTAP SMB-Servern . . . 293
Aktivieren und Deaktivieren von BranchCache . . . 297
Die BranchCache Konfiguration verwalten und überwachen . . . 306
Verbesserung der Microsoft Remote Copy Leistung . . . 318
Die Client-Antwortzeit wird durch die Bereitstellung von SMB automatischen Knotenverweisen mit Auto Location verbessert. . . . 324
Ordnersicherheit auf Freigaben mit zugriffsbasierter Aufzählung bereitstellen . . . 331
Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen bei NFS und SMB . . . 334
Informationen zu den Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen in ONTAP NFS und SMB . . . 334

Informationen zu gültigen Zeichen für ONTAP SMB Datei- oder Verzeichnisnamen 334
Groß-/Kleinschreibung von ONTAP SMB Datei- und Verzeichnisnamen in einer Multiprotokollumgebung 334
Informationen zur Erstellung von ONTAP SMB Datei- und Verzeichnisnamen 335
Informationen zu ONTAP SMB Multibyte-Datei-, Verzeichnis- und Qtree-Namen 336
Zeichenzuordnung für die ONTAP SMB-Dateinamenübersetzung auf Volumes konfigurieren 337
ONTAP Befehle zur Verwaltung von Zeichenzuordnungen für die SMB-Dateinamenübersetzung 339

SMB mit der Befehlszeile verwalten

Informationen zu ONTAP SMB

ONTAP Dateizugriffsfunktionen sind für das SMB-Protokoll verfügbar. Ein CIFS-Server kann aktiviert, Freigaben können erstellt und Microsoft-Dienste aktiviert werden.

SMB (Server Message Block) bezeichnet moderne Dialekte des Common Internet File System (CIFS)-Protokolls. *CIFS* erscheint weiterhin in der ONTAP-Befehlszeilenschnittstelle (CLI) und in OnCommand Management-Tools.

SMB Server-Unterstützung

Informationen zur Unterstützung von ONTAP SMB-Servern

Sie können SMB-Server auf Storage Virtual Machines (SVMs) aktivieren und konfigurieren, um SMB-Clients den Zugriff auf Dateien in Ihrem Cluster zu ermöglichen.

- Jede Daten-SVM im Cluster kann genau einer Active Directory Domäne zugeordnet werden.
- Daten-SVMs müssen nicht an dieselbe Domäne gebunden sein.
- Mehrere SVMs können an denselben Bereich gebunden werden.

Sie müssen die SVMs und LIFs, die Sie zur Datenbereitstellung verwenden, konfigurieren, bevor Sie einen SMB-Server erstellen können. Wenn Ihr Datennetzwerk nicht flach ist, müssen möglicherweise auch IPspaces, Broadcast-Domänen und Subnetze konfiguriert werden.

Verwandte Informationen

"Netzwerkmanagement"

Server modifizieren

"Systemadministration"

Unterstützte ONTAP SMB Versionen und Funktionen

Server Message Block (SMB) ist ein Remote-Dateifreigabeprotokoll, das von Microsoft Windows Clients und Servern verwendet wird. ONTAP unterstützt alle SMB-Versionen. Sie sollten überprüfen, ob der ONTAP SMB-Server die in Ihrer Umgebung erforderlichen Clients und Funktionen unterstützt.

Die aktuellsten Informationen darüber, welche SMB-Clients und Domänencontroller ONTAP unterstützt, sind im *Interoperability Matrix Tool* verfügbar.

SMB 2.0 und spätere Versionen sind für ONTAP SMB Server standardmäßig aktiviert und können je nach Bedarf aktiviert oder deaktiviert werden. Ebenso kann SMB 1.0 je nach Bedarf aktiviert oder deaktiviert werden.

Ab ONTAP 9.20.1 unterstützt ONTAP SMB-Namensabfragen mit normalisierten Namen für geöffnete Dateien und Verzeichnisse. Windows-Clients können kanonische Datei- und Verzeichnisnamen in einer einzigen

Anforderung abrufen.

> Die Standardeinstellungen für SMB 1.0- und 2.0-Verbindungen zu Domänencontrollern hängen ebenfalls von der ONTAP Version ab. Weitere Informationen zum `vserver cifs security modify` Befehl finden Sie in der "ONTAP-Befehlsreferenz". Für Umgebungen mit vorhandenen CIFS-Servern, auf denen SMB 1.0 ausgeführt wird, empfiehlt NetApp so bald wie möglich die Migration auf eine neuere SMB-Version, um sich auf Verbesserungen bei Sicherheit und Compliance vorzubereiten. Einzelheiten erhalten Sie bei Ihrem NetApp Ansprechpartner.

Die folgende Tabelle zeigt, welche SMB-Funktionen in den einzelnen SMB-Versionen unterstützt werden. Einige SMB-Funktionen sind standardmäßig aktiviert und einige erfordern eine zusätzliche Konfiguration.

Diese Funktionalität:	**Erfordert Aktivierung:**	**Wird in ONTAP 9 für diese SMB-Versionen unterstützt:**	
		3,0	3.1.1
Legacy SMB 1.0 Funktionalität		X	X
Robuste Griffe		X	X
Zusammengesetzte Operationen		X	X
Asynchrone Operationen		X	X
Vergrößerte Lese- und Schreibpuffergrößen		X	X
Erhöhte Skalierbarkeit		X	X
SMB-Signierung	X	X	X
Alternate Data Stream (ADS) Dateiformat	X	X	X
Große MTU (standardmäßig aktiviert ab ONTAP 9.7)	X	X	X
Lease-Oplocks		X	X
Ständig verfügbare Freigaben	X	X	X
Persistente Handles		X	X
Zeuge		X	X
SMB-Verschlüsselung: AES-128-CCM	X	X	X
Scale out (erforderlich für CA-Shares)		X	X
Transparente Ausfallsicherung		X	X
SMB Multichannel (beginnend mit ONTAP 9.4)	X	X	X

Diese Funktionalität:	Erfordert Aktivierung:	Wird in ONTAP 9 für diese SMB-Versionen unterstützt:	
Integrität vor der Authentifizierung			X
Cluster Client Failover v.2 (CCFv2)			X
SMB-Verschlüsselung: AES-128-GCM	X		X
Unterstützung für normalisierte Namensabfragen für Windows-Clients (ab ONTAP 9.20.1)		X	X

Verwandte Informationen

Informationen zur Verwendung von ONTAP Signaturen zur Verbesserung der Netzwerksicherheit

Minimales Sicherheit bei der Authentifizierung-Niveau des Servers festlegen

Erforderliche SMB-Verschlüsselung auf SMB-Servern für Datentransfers über SMB konfigurieren

"NetApp Interoperabilität"

Nicht unterstützte Windows-Funktionen in ONTAP SMB

Bevor Sie CIFS in Ihrem Netzwerk verwenden, müssen Sie sich über bestimmte Windows-Funktionen im Klaren sein, die ONTAP nicht unterstützt.

ONTAP unterstützt die folgenden Windows-Funktionen nicht:

- Verschlüsseltes Dateisystem (EFS)
- Protokollierung von NT File System (NTFS)-Ereignissen im Änderungsjournal
- Microsoft File Replication Service (FRS)
- Microsoft Windows Indexing Service
- Remote-Speicherung durch Hierarchical Storage Management (HSM)
- Kontingentverwaltung von Windows-Clients
- Windows Kontingensemantik
- Die LMHOSTS-Datei
- NTFS native Komprimierung

NIS- oder LDAP-Namensdienste auf ONTAP SMB SVMs konfigurieren

Bei SMB-Zugriff wird die Zuordnung zu einem UNIX-Benutzer immer durchgeführt, auch beim Zugriff auf Daten in einem NTFS Security-Style-Volume. Wenn Windows-Benutzer entsprechenden UNIX-Benutzern zugeordnet werden, deren Informationen in NIS- oder LDAP-Verzeichnisdiensten gespeichert sind, oder wenn LDAP für die Namenszuordnung

verwendet wird, empfiehlt es sich, diese Namensdienste während der SMB-Einrichtung zu konfigurieren.

Bevor Sie beginnen

Die Konfiguration Ihrer Name Services-Datenbank muss an Ihre Namensdienstinfrastruktur angepasst worden sein.

Über diese Aufgabe

SVMs verwenden die ns-switch-Datenbanken der Namensdienste, um die Reihenfolge festzulegen, in der die Quellen für eine bestimmte Namensdienste-Datenbank abgefragt werden. Die ns-switch-Quelle kann eine beliebige Kombination aus `files`, `nis` oder `ldap` sein. Für die groups-Datenbank versucht ONTAP, die Gruppenmitgliedschaften von allen konfigurierten Quellen abzurufen und verwendet anschließend die konsolidierten Gruppenmitgliedschaftsinformationen für Zugriffsprüfungen. Ist eine dieser Quellen zum Zeitpunkt des Abrufs der UNIX-Gruppeninformationen nicht verfügbar, kann ONTAP die vollständigen UNIX-Anmeldeinformationen nicht abrufen und nachfolgende Zugriffsprüfungen könnten fehlschlagen. Es sollte immer sichergestellt sein, dass alle ns-switch-Quellen für die groups-Datenbank in den ns-switch-Einstellungen konfiguriert sind.

Standardmäßig ordnet der SMB-Server alle Windows-Benutzer dem in der lokalen `passwd` Datenbank gespeicherten Standard-UNIX-Benutzer zu. Bei Verwendung der Standardkonfiguration ist die Konfiguration von NIS- oder LDAP-Diensten für UNIX-Benutzer- und Gruppennamen oder der LDAP-Benutzerzuordnung für den SMB-Zugriff optional.

Schritte

1. Wenn UNIX-Benutzer-, Gruppen- und Netzgruppeninformationen von NIS-Namensdiensten verwaltet werden, sind die NIS-Namensdienste zu konfigurieren:

   a. Die aktuelle Reihenfolge der Namensdienste lässt sich mit dem `vserver services name-service ns-switch show` Befehl feststellen.

      In diesem Beispiel verwenden die drei Datenbanken (`group`, `passwd` und `netgroup`), die `nis` als Namensdienstquelle nutzen können, nur `files` als Quelle.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                   Source
      Vserver         Database       Enabled       Order
      --------------- ------------   ---------     ---------
      vs1             hosts          true          dns,
                                                   files
      vs1             group          true          files
      vs1             passwd         true          files
      vs1             netgroup       true          files
      vs1             namemap        true          files
      ```

      Sie müssen die `nis`Quelle zu der `group` und `passwd`Datenbank sowie optional zur `netgroup`Datenbank hinzufügen.

   b. Passen Sie die Reihenfolge der Namensdienst-Datenbank ns-switch nach Bedarf mit dem `vserver services name-service ns-switch modify` Befehl an.

Für eine optimale Leistung sollte ein Namensdienst nur dann zu einer Namensdienstdatenbank hinzugefügt werden, wenn geplant ist, diesen Namensdienst auf der SVM zu konfigurieren.

Wenn Sie die Konfiguration für mehr als eine Namensdienstdatenbank ändern, muss der Befehl für jede Namensdienstdatenbank, die geändert werden soll, separat ausgeführt werden.

In diesem Beispiel sind `nis` und `files` als Quellen für die `group` und `passwd` Datenbanken in dieser Reihenfolge konfiguriert. Die übrigen Namensdienstdatenbanken bleiben unverändert.

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. Es kann überprüft werden, ob die Reihenfolge der Namensdienste korrekt ist, indem der `vserver services name-service ns-switch show` Befehl verwendet wird.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. Die NIS-Namensdienstkonfiguration erstellen:
`vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…`

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

> Das Feld `-nis-servers` ersetzte das Feld `-servers`. Dieses Feld kann entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server enthalten.

e. Es sollte überprüft werden, ob der NIS-Namensdienst ordnungsgemäß konfiguriert ist: `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Server
------------- ------------------- ---------------
```

```
vs1             example.com          10.0.0.60
```

2. Wenn UNIX-Benutzer-, Gruppen- und Netzgruppeninformationen oder Namenszuordnungen über LDAP-Namensdienste verwaltet werden, ist die Konfiguration der LDAP-Namensdienste mit den Informationen vorzunehmen, die sich unter "NFS Management" befinden.

Informationen zur Konfiguration des ONTAP SMB Name Service Switch

ONTAP speichert Konfigurationsinformationen für den Namensdienst in einer Tabelle, die der `/etc/nsswitch.conf` Datei auf UNIX-Systemen entspricht. Die Funktion dieser Tabelle und die Nutzung durch ONTAP sind zu verstehen, damit eine angemessene Konfiguration für die jeweilige Umgebung möglich ist.

Die ONTAP Name Service Switch-Tabelle legt fest, welche Namensdienstquellen ONTAP in welcher Reihenfolge abruft, um Informationen für einen bestimmten Typ von Namensdienstinformationen zu erhalten. ONTAP führt für jede SVM eine separate Name Service Switch-Tabelle.

Datenbanktypen

Die Tabelle speichert eine separate Namensdienstliste für jeden der folgenden Datenbanktypen:

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Hosts	Umwandlung von Hostnamen in IP-Adressen	Dateien, DNS
Gruppe	Benutzergruppeninformationen abrufen	Dateien, NIS, LDAP
passwd	Benutzerinformationen abrufen	Dateien, NIS, LDAP
Netgroup	Netgroup-Informationen nachschlagen	Dateien, NIS, LDAP
Namenszuordnung	Zuordnung von Benutzernamen	Dateien, LDAP

Quellentypen

Die Quellen geben an, welche Namensdienstquelle für das Abrufen der entsprechenden Informationen verwendet wird.

Quelltyp angeben…	Informationen können nachgeschlagen werden in…	Verwaltet von den Kommandofamilien…

Dateien	Lokale Quelldateien	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Externe NIS-Server wie in der NIS-Domänenkonfiguration der SVM angegeben	`vserver services name-service nis-domain`
LDAP	Externe LDAP-Server, wie in der LDAP-Client-Konfiguration der SVM angegeben	`vserver services name-service ldap`
DNS	Externe DNS-Server wie in der DNS-Konfiguration der SVM angegeben	`vserver services name-service dns`

Auch wenn geplant ist, NIS oder LDAP sowohl für den Datenzugriff als auch für die SVM-Administrationsauthentifizierung zu verwenden, sollten `files`lokale Benutzer dennoch als Fallback einbezogen und konfiguriert werden, falls die NIS- oder LDAP-Authentifizierung fehlschlägt.

Protokolle für den Zugriff auf externe Quellen

Für den Zugriff auf die Server externer Quellen verwendet ONTAP die folgenden Protokolle:

Externe Namensdienstquelle	Für den Zugriff verwendetes Protokoll
NIS	UDP
DNS	UDP
LDAP	TCP

Beispiel

Das folgende Beispiel zeigt die Konfiguration des Namensdienstschalters für die SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
```

```
svm_1           netgroup       nis,
                               files
```

Um Benutzer- oder Gruppeninformationen abzurufen, konsultiert ONTAP ausschließlich lokale Quelldateien. Liefert die Abfrage keine Ergebnisse, schlägt die Suche fehl.

Um Informationen zu Netzgruppen abzurufen, konsultiert ONTAP zunächst externe NIS-Server. Falls die Abfrage keine Ergebnisse liefert, wird anschließend die lokale Netzgruppendatei überprüft.

Für die SVM svm_1 sind in der Tabelle keine Namensdiensteinträge für die Namenszuordnung vorhanden. Daher konsultiert ONTAP standardmäßig nur lokale Quelldateien.

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` b. `vserver cifs options modify -vserver` *`vserver_name options`* 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`
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,...]` 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.
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,...]` 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

Oplock-Status überwachen

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` Sie können zusätzliche Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste angeben. 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` Sie können zusätzliche zu entfernende Freigabeeigenschaften mit einer durch Kommas getrennten Liste angeben. 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 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`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
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` *LIF_IP_address* ist die IPv6-Adresse des Daten-LIF.

SMB Server-Sicherheitseinstellungen verwalten

Informationen zur Handhabung der ONTAP SMB Client-Authentifizierung

Bevor Benutzer SMB-Verbindungen herstellen können, um auf Daten auf der SVM zuzugreifen, müssen sie von der Domäne, zu der der SMB-Server gehört, authentifiziert werden. Der SMB-Server unterstützt zwei Authentifizierungsmethoden: Kerberos und NTLM (NTLMv1 oder NTLMv2). Kerberos ist die Standardmethode zur Authentifizierung von Domänenbenutzern.

Kerberos-Authentifizierung

ONTAP unterstützt die Kerberos-Authentifizierung beim Erstellen authentifizierter SMB-Sitzungen.

Kerberos ist der primäre Authentifizierungsdienst für Active Directory. Der Kerberos-Server oder Kerberos Key Distribution Center (KDC) Dienst speichert und ruft Informationen über Sicherheitsprinzipale im Active Directory ab. Im Gegensatz zum NTLM-Modell kontaktieren Active Directory Clients, die eine Sitzung mit einem anderen Computer wie dem SMB Server herstellen möchten, direkt einen KDC, um ihre Sitzungsberechtigungen zu erhalten.

NTLM-Authentifizierung

Die NTLM Client-Authentifizierung erfolgt mittels eines Challenge-Response-Protokolls, das auf dem gemeinsamen Wissen über ein benutzerspezifisches Geheimnis basiert, welches wiederum auf einem Passwort beruht.

Wenn ein Benutzer eine SMB-Verbindung mit einem lokalen Windows-Benutzerkonto herstellt, erfolgt die Authentifizierung lokal durch den SMB-Server mittels NTLMv2.

Informationen zu den SMB-Server-Sicherheitseinstellungen für die ONTAP SVM-Disaster Recovery Konfiguration

Bevor eine SVM erstellt wird, die als Disaster Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (die `-identity-preserve` Option ist auf `false` in der SnapMirror-Konfiguration gesetzt), ist es wichtig, Informationen darüber zu haben, wie die SMB-Server-Sicherheitseinstellungen auf der Ziel-SVM verwaltet werden.

- Nicht standardmäßige SMB-Server-Sicherheitseinstellungen werden nicht auf das Ziel repliziert.

  Beim Erstellen eines SMB-Servers auf der Ziel-SVM werden alle Sicherheitseinstellungen des SMB-Servers auf die Standardwerte gesetzt. Bei der Initialisierung, Aktualisierung oder Resynchronisierung der SVM für die Notfallwiederherstellung werden die Sicherheitseinstellungen des SMB-Servers auf der Quelle nicht auf das Ziel repliziert.

- Die von den Standardeinstellungen abweichenden Sicherheitseinstellungen des SMB-Servers sind manuell zu konfigurieren.

  Wenn auf der Quell-SVM nicht standardmäßige SMB-Server-Sicherheitseinstellungen konfiguriert sind, müssen diese Einstellungen auf der Ziel-SVM manuell konfiguriert werden, nachdem die Ziel-SVM Lese- und Schreibzugriff erhält (nachdem die SnapMirror Beziehung aufgehoben wurde).

Informationen zu den Sicherheitseinstellungen des ONTAP SMB-Servers anzeigen

Informationen zu den Sicherheitseinstellungen des SMB-Servers auf den Storage Virtual Machines (SVMs) können angezeigt werden. Diese Informationen ermöglichen die Überprüfung, ob die Sicherheitseinstellungen korrekt sind.

Über diese Aufgabe

Eine angezeigte Sicherheitseinstellung kann der Standardwert für dieses Objekt oder ein nicht standardmäßiger Wert sein, der entweder über die ONTAP CLI oder über Active Directory Gruppenrichtlinienobjekte (GPOs) konfiguriert wird.

Der `vserver cifs security show` Befehl sollte für SMB-Server im Arbeitsgruppenmodus nicht verwendet werden, da einige Optionen ungültig sind.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
Alle Sicherheitseinstellungen auf einer bestimmten SVM	`vserver cifs security show -vserver` *`vserver_name`*
Eine oder mehrere spezifische Sicherheitseinstellungen auf dem SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]`Sie können `-fields ?` eingeben, um festzustellen, welche Felder Sie verwenden können.

Beispiel

Das folgende Beispiel zeigt alle Sicherheitseinstellungen für SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
         Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Beachten Sie, dass die angezeigten Einstellungen von der ausgeführten ONTAP Version abhängen.

Das folgende Beispiel zeigt die Kerberos-Taktabweichung für SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Verwandte Informationen

Informationen zu GPO-Konfigurationen anzeigen

ONTAP Passwortkomplexität für lokale SMB-Benutzer konfigurieren

Die erforderliche Passwortkomplexität bietet erhöhte Sicherheit für lokale SMB-Benutzer auf Ihren Storage Virtual Machines (SVMs). Die Funktion für erforderliche Passwortkomplexität ist standardmäßig aktiviert. Sie kann jederzeit deaktiviert und wieder aktiviert werden.

Bevor Sie beginnen

Lokale Benutzer, lokale Gruppen und die lokale Benutzerauthentifizierung müssen auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Der `vserver cifs security modify` Befehl sollte für einen CIFS-Server im Arbeitsgruppenmodus nicht verwendet werden, da einige Optionen ungültig sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn eine erforderliche Passwortkomplexität für lokale SMB-Benutzer gelten soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Deaktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Die Sicherheitseinstellung für die erforderliche Passwortkomplexität überprüfen: `vserver cifs security show -vserver` *`vserver_name`*

Beispiel

Das folgende Beispiel zeigt, dass die erforderliche Kennwortkomplexität für lokale SMB-Benutzer für SVM vs1 aktiviert ist:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Verwandte Informationen

- Informationen zu den Server-Sicherheitseinstellungen
- Informationen zu lokalen Benutzern und Gruppen
- Anforderungen an lokale Benutzerpasswörter
- Passwörter lokaler Benutzerkonten ändern

Die Kerberos-Sicherheitseinstellungen des ONTAP SMB-Servers ändern

Sie können bestimmte Kerberos-Sicherheitseinstellungen des CIFS-Servers ändern, darunter die maximal zulässige Kerberos-Uhrzeitabweichung, die Lebensdauer des

Kerberos-Tickets und die maximale Anzahl der Ticketverlängerungstage.

Über diese Aufgabe

Die Änderung der Kerberos-Einstellungen eines CIFS-Servers mittels des `vserver cifs security modify` Befehls ändert die Einstellungen nur auf der einzelnen Storage Virtual Machine (SVM), die Sie mit dem `-vserver` Parameter angeben. Die Kerberos-Sicherheitseinstellungen für alle SVMs im Cluster, die zur selben Active Directory Domäne gehören, können zentral über Active Directory Gruppe Policy Objects (GPOs) verwaltet werden.

Schritte

1. Eine oder mehrere der folgenden Aktionen können durchgeführt werden:

Wenn Sie möchten…	Eingeben…
Die maximal zulässige Kerberos-Uhrzeitabweichung in Minuten (9.13.1 und später) oder Sekunden (9.12.1 oder früher) angeben.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* Die Standardeinstellung beträgt 5 Minuten.
Die Lebensdauer des Kerberos-Tickets in Stunden angeben.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` Die Standardeinstellung beträgt 10 Stunden.
Die maximale Anzahl der Tage für die Ticketverlängerung angeben.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* Die Standardeinstellung beträgt 7 Tage.
Geben Sie die Zeitüberschreitung für Sockets auf KDCs an, nach der alle KDCs als nicht erreichbar markiert werden.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* Die Standardeinstellung beträgt 3 Sekunden.

2. Die Kerberos-Sicherheitseinstellungen überprüfen:

   `vserver cifs security show -vserver` *`vserver_name`*

Beispiel

Das folgende Beispiel nimmt die folgenden Änderungen an der Kerberos-Sicherheit vor: “Kerberos Clock Skew” wird auf 3 Minuten und “Kerberos Ticket Age” auf 8 Stunden für SVM vs1 gesetzt:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1
```

```
                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                 false
        Is Password Complexity Required:                  true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

Verwandte Informationen

"Informationen zu den Server-Sicherheitseinstellungen"

"Unterstützte Gruppenrichtlinienobjekte"

"Anwenden von Gruppenrichtlinienobjekten auf CIFS-Server"

Das minimale Sicherheit bei der Authentifizierung Niveau des ONTAP SMB-Servers festlegen

Sie können die minimale Sicherheitsstufe des SMB-Servers, auch bekannt als *LMCompatibilityLevel*, auf Ihrem SMB-Server festlegen, um die Sicherheitsanforderungen Ihres Unternehmens für den SMB-Clientzugriff zu erfüllen. Die minimale Sicherheitsstufe ist die Mindeststufe der Sicherheitstoken, die der SMB-Server von SMB-Clients akzeptiert.

Über diese Aufgabe

- SMB-Server im Arbeitsgruppenmodus unterstützen ausschließlich NTLM-Authentifizierung. Kerberos-Authentifizierung wird nicht unterstützt.
- LMCompatibilityLevel gilt nur für die SMB-Client-Authentifizierung, nicht für die Administrator-Authentifizierung.

Das minimale Sicherheit bei der Authentifizierung kann auf eines von vier unterstützten Sicherheitsniveaus festgelegt werden.

Wert	Beschreibung
`lm-ntlm-ntlmv2-krb` (Standard)	Die Storage Virtual Machine (SVM) akzeptiert LM-, NTLM-, NTLMv2- und Kerberos-Sicherheit bei der Authentifizierung.
`ntlm-ntlmv2-krb`	Die SVM akzeptiert NTLM-, NTLMv2- und Kerberos-Sicherheit bei der Authentifizierung. Die SVM lehnt LM-Authentifizierung ab.
`ntlmv2-krb`	Die SVM akzeptiert NTLMv2 und Kerberos Sicherheit bei der Authentifizierung. Die SVM lehnt LM und NTLM Authentifizierung ab.

Wert	Beschreibung
`krb`	Die SVM akzeptiert ausschließlich Kerberos-Sicherheit bei der Authentifizierung. Die SVM verweigert LM-, NTLM- und NTLMv2-Authentifizierung.

Schritte

1. Minimales Sicherheitsniveau bei der Authentifizierung festlegen: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Es sollte sichergestellt sein, dass die Sicherheit bei der Authentifizierung auf das gewünschte Niveau eingestellt ist: `vserver cifs security show -vserver vserver_name`

Verwandte Informationen

AES-Verschlüsselung für Kerberos-basierte Kommunikation konfigurieren

Starke ONTAP SMB-Sicherheit für Kerberos-basierte Kommunikation mit AES-Verschlüsselung konfigurieren

Für maximale Sicherheit bei Kerberos-basierter Kommunikation kann die AES-256- und AES-128-Verschlüsselung auf dem SMB-Server aktiviert werden. Standardmäßig ist beim Erstellen eines SMB-Servers auf der SVM die Advanced Encryption Standard (AES)-Verschlüsselung deaktiviert. Eine Aktivierung ist erforderlich, um von der starken Sicherheit der AES-Verschlüsselung zu profitieren.

Die Kerberos-bezogene Kommunikation für SMB wird sowohl bei der Erstellung des SMB-Servers auf der SVM als auch während der Einrichtung der SMB-Sitzung verwendet. Der SMB-Server unterstützt die folgenden Verschlüsselungstypen für die Kerberos-Kommunikation:

- AES 256
- AES 128
- DES
- RC4-HMAC

Wenn die höchste Sicherheitsverschlüsselungsart für die Kerberos-Kommunikation verwendet werden soll, sollte die AES-Verschlüsselung für die Kerberos-Kommunikation auf der SVM aktiviert werden.

Bei der Erstellung des SMB-Servers legt der Domänencontroller ein Computerkonto in Active Directory an. Zu diesem Zeitpunkt erkennt der KDC die Verschlüsselungsfunktionen dieses Computerkontos. Anschließend wird ein bestimmter Verschlüsselungstyp für die Verschlüsselung des Diensttickets ausgewählt, das der Client dem Server während der Authentifizierung vorlegt.

Ab ONTAP 9.12.1 kann festgelegt werden, welche Verschlüsselungstypen dem Active Directory (AD) KDC bekanntgegeben werden. Die `-advertised-enc-types` Option kann verwendet werden, um empfohlene Verschlüsselungstypen zu aktivieren und schwächere Verschlüsselungstypen zu deaktivieren. Informationen dazu, wie "AES-Verschlüsselung für Kerberos-basierte Kommunikation konfigurieren".

Intel AES New Instructions (Intel AES NI) ist in SMB 3.0 verfügbar, verbessert den AES-Algorithmus und beschleunigt die Datenverschlüsselung mit unterstützten Prozessorfamilien. Ab

SMB 3.1.1 ersetzt AES-128-GCM AES-128-CCM als den von der SMB-Verschlüsselung verwendeten Hash-Algorithmus.

Verwandte Informationen

Die Server-Sicherheitseinstellungen anpassen

AES-Verschlüsselung für die Kerberos-basierte Kommunikation von ONTAP SMB konfigurieren

Um die maximale Sicherheit bei der Kerberos-basierten Kommunikation zu gewährleisten, sollte auf dem SMB-Server die AES-256- und AES-128-Verschlüsselung verwendet werden. Ab ONTAP 9.13.1 ist die AES-Verschlüsselung standardmäßig aktiviert. Wenn nicht gewünscht ist, dass der SMB-Server die AES-Verschlüsselungstypen für die Kerberos-basierte Kommunikation mit dem Active Directory (AD) KDC auswählt, kann die AES-Verschlüsselung deaktiviert werden.

Ob die AES-Verschlüsselung standardmäßig aktiviert ist und ob Sie die Möglichkeit haben, Verschlüsselungstypen anzugeben, hängt von Ihrer ONTAP Version ab.

ONTAP Version	AES-Verschlüsselung ist aktiviert …	Es können Verschlüsselungstypen angegeben werden.
9.13.1 und später	Standardmäßig	Ja
9.12.1	Manuell	Ja
9.11.1 und früher	Manuell	Nein

Ab ONTAP 9.12.1 wird die AES-Verschlüsselung mit der `-advertised-enc-types` Option aktiviert und deaktiviert, wodurch die an den AD KDC gemeldeten Verschlüsselungstypen festgelegt werden können. Die Standardeinstellung ist `rc4` und `des`, aber wenn ein AES-Typ angegeben wird, ist die AES-Verschlüsselung aktiviert. Mit der Option kann außerdem explizit das Deaktivieren der schwächeren Verschlüsselungstypen RC4 und DES erfolgen. In ONTAP 9.11.1 und früher muss die `-is-aes-encryption-enabled` Option verwendet werden, um die AES-Verschlüsselung zu aktivieren und zu deaktivieren; die Verschlüsselungstypen können dabei nicht angegeben werden.

Wenn der `-advertised-enc-types` Parameter geändert wird, ersetzen die angegebenen Verschlüsselungstypen alle zuvor konfigurierten Typen. Alle vorherigen Einstellungen für Verschlüsselungstypen werden entfernt.

Zur Erhöhung der Sicherheit ändert die Storage Virtual Machine (SVM) ihr Maschinenkontokennwort im AD jedes Mal, wenn die AES-Sicherheitsoption geändert wird. Für die Kennwortänderung sind möglicherweise administrative AD-Anmeldeinformationen für die Organisationseinheit (OU) erforderlich, die das Maschinenkonto enthält. Eine Anmeldeaufforderung erscheint nur, wenn ONTAP das Maschinenkontokennwort im Active Directory zurücksetzen muss und Ihre AD-Konfiguration administrative Anmeldeinformationen für die Organisationseinheit erfordert, die das Maschinenkonto enthält. Wenn Ihr AD synchronisiert ist und die automatische Zurücksetzung aktiviert ist, erscheint keine Aufforderung.

Wenn eine SVM als Disaster-Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (die `-identity-preserve` Option ist auf `false` in der SnapMirror-Konfiguration gesetzt), werden die nicht standardmäßigen SMB-Server-Sicherheitseinstellungen nicht auf das Ziel repliziert. Ist die AES-Verschlüsselung auf der Quell-SVM aktiviert, muss sie manuell aktiviert werden.

Beispiel 1. Schritte

ONTAP 9.12.1 und höher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die AES-Verschlüsselungstypen für die Kerberos-Kommunikation verwendet werden sollen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Hinweis: Die `-is-aes-encryption-enabled` Option ist in ONTAP 9.12.1 veraltet und könnte in einer späteren Version entfernt werden.

2. Es kann überprüft werden, ob die AES-Verschlüsselung wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Beispiele

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2. Der Administrator wird aufgefordert, die administrativen AD-Anmeldeinformationen für die OU einzugeben, die den SMB-Server enthält.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".
```

```
Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 und früher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die AES-Verschlüsselungstypen für die Kerberos-Kommunikation verwendet werden sollen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Es kann überprüft werden, ob die AES-Verschlüsselung wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Das `is-aes-encryption-enabled` Feld zeigt `true` an, wenn die AES-Verschlüsselung aktiviert ist, und `false` wenn sie deaktiviert ist.

Beispiele

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2. Der Administrator wird aufgefordert, die administrativen AD-Anmeldeinformationen für die OU einzugeben, die

den SMB-Server enthält.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Verwandte Informationen

"Domänenbenutzer kann sich nicht im Cluster mit Domain-Tunnel anmelden"

SMB-Signierung zur Erhöhung der Netzwerksicherheit verwenden

Informationen zur Verwendung von ONTAP SMB-Signaturen zur Verbesserung der Netzwerksicherheit

Die SMB-Signierung trägt dazu bei, sicherzustellen, dass der Netzwerkverkehr zwischen dem SMB-Server und dem Client nicht kompromittiert wird; dies geschieht durch die Verhinderung von Replay-Angriffen. Standardmäßig unterstützt ONTAP die SMB-Signierung, wenn sie vom Client angefordert wird. Optional kann der Speicheradministrator den SMB-Server so konfigurieren, dass die SMB-Signierung erforderlich ist.

Wie sich Signaturrichtlinien auf die Kommunikation mit ONTAP SMB-Servern auswirken

Zusätzlich zu den SMB-Signatur-Sicherheitseinstellungen des CIFS-Servers steuern zwei SMB-Signaturrichtlinien auf Windows-Clients die digitale Signatur der Kommunikation zwischen Clients und dem CIFS-Server. Es kann die Einstellung konfiguriert werden, die den Geschäftsanforderungen entspricht.

Die SMB-Clientrichtlinien werden über die lokalen Sicherheitsrichtlinieneinstellungen von Windows gesteuert, die mithilfe der Microsoft Management Console (MMC) oder Active Directory GPOs konfiguriert werden. Weitere Informationen zur SMB-Clientsignierung und zu Sicherheitsproblemen enthält die Microsoft Windows-Dokumentation.

Hier sind Beschreibungen der beiden SMB-Signaturrichtlinien auf Microsoft Clients:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Diese Einstellung steuert, ob die SMB-Signaturfunktion des Clients aktiviert ist. Sie ist standardmäßig aktiviert. Wenn diese Einstellung auf dem Client deaktiviert ist, hängt die Kommunikation des Clients mit dem CIFS-Server von der SMB-Signatureinstellung auf dem CIFS-Server ab.

- `Microsoft network client: Digitally sign communications (always)`

  Diese Einstellung steuert, ob der Client für die Kommunikation mit einem Server eine SMB-Signatur benötigt. Sie ist standardmäßig deaktiviert. Wenn diese Einstellung auf dem Client deaktiviert ist, richtet sich das Verhalten bei der SMB-Signatur nach der Richtlinieneinstellung für `Microsoft network client: Digitally sign communications (if server agrees)` und der Einstellung auf dem CIFS-Server.

> Wenn Ihre Umgebung Windows-Clients umfasst, die so konfiguriert sind, dass sie SMB-Signierung erfordern, muss die SMB-Signierung auf dem CIFS-Server aktiviert werden. Andernfalls kann der CIFS-Server diesen Systemen keine Daten bereitstellen.

Die effektiven Ergebnisse der SMB-Signatureinstellungen von Client und CIFS-Server hängen davon ab, ob die SMB-Sitzungen SMB 1.0 oder SMB 2.x und höher verwenden.

Die folgende Tabelle fasst das effektive SMB-Signaturverhalten zusammen, wenn die Sitzung SMB 1.0 verwendet:

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Signieren deaktiviert und nicht erforderlich	Nicht unterschrieben	Unterzeichnet
Signierung aktiviert und nicht erforderlich	Nicht unterschrieben	Unterzeichnet
Signieren deaktiviert und erforderlich	Unterzeichnet	Unterzeichnet
Signierung aktiviert und erforderlich	Unterzeichnet	Unterzeichnet

> Ältere Windows SMB 1 Clients und einige Nicht-Windows SMB 1 Clients können möglicherweise keine Verbindung herstellen, wenn die Signierung auf dem Client deaktiviert ist, aber auf dem CIFS-Server erforderlich ist.

Die folgende Tabelle fasst das effektive SMB-Signaturverhalten zusammen, wenn die Sitzung SMB 2.x oder SMB 3.0 verwendet:

> Für SMB 2.x und SMB 3.0 Clients ist die SMB-Signierung immer aktiviert. Sie kann nicht deaktiviert werden.

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Unterschrift nicht erforderlich	Nicht unterschrieben	Unterzeichnet

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Unterschrift erforderlich	Unterzeichnet	Unterzeichnet

Die folgende Tabelle fasst das Standardverhalten von Microsoft-Client und -Server bei der SMB-Signierung zusammen:

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Kann erforderlich sein/nicht erforderlich sein	Client-Standard	Serverstandard	DC Standard
SMB 1.0	MD5	Ja	Ja	Aktiviert (nicht erforderlich)	Deaktiviert (nicht erforderlich)	Erforderlich
SMB 2.x	HMAC SHA-256	Nein	Ja	Nicht erforderlich	Nicht erforderlich	Erforderlich
SMB 3.0	AES-CMAC.	Nein	Ja	Nicht erforderlich	Nicht erforderlich	Erforderlich

Microsoft empfiehlt nicht mehr, `Digitally sign communications (if client agrees)` oder `Digitally sign communications (if server agrees)` Gruppenrichtlinieneinstellungen zu verwenden. Microsoft empfiehlt außerdem nicht mehr, die `EnableSecuritySignature` Registrierungseinstellungen zu verwenden. Diese Optionen betreffen nur das SMB 1 Verhalten und können durch die `Digitally sign communications (always)` Gruppenrichtlinieneinstellung oder die `RequireSecuritySignature` Registrierungseinstellung ersetzt werden.

Informationen zu den Auswirkungen der ONTAP SMB-Signatur auf die Leistung

Wenn SMB-Sitzungen SMB-Signatur verwenden, kommt es zu Leistungseinbußen bei der gesamten SMB-Kommunikation mit Windows-Clients, was sowohl die Clients als auch den Server betrifft (also die Knoten im Cluster, auf denen die SVM mit dem SMB-Server ausgeführt wird).

Die Auswirkungen auf die Leistung zeigen sich in einer erhöhten CPU-Auslastung sowohl auf den Clients als auch auf dem Server, obwohl sich das Netzwerkverkehr nicht ändert.

Das Ausmaß der Leistungseinbußen hängt von der Version von ONTAP 9 ab, die Sie verwenden. Ab ONTAP 9.7 kann ein neuer Verschlüsselungs-Offload-Algorithmus eine bessere Performance bei signiertem SMB-Datenverkehr ermöglichen. SMB-Signatur-Offload ist standardmäßig aktiviert, wenn die SMB-Signierung aktiviert ist.

Für eine verbesserte SMB-Signaturleistung ist die AES-NI-Offload-Funktion erforderlich. Im Hardware Universe (HWU) kann überprüft werden, ob für Ihre Plattform AES-NI-Offload unterstützt wird.

Weitere Leistungsverbesserungen sind ebenfalls möglich, wenn Sie SMB Version 3.11 verwenden können, die den wesentlich schnelleren GCM Algorithmus unterstützt.

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung kann der Einfluss der SMB-

Signierung auf die Leistung stark variieren; dies lässt sich nur durch Tests in Ihrer Netzwerkumgebung überprüfen.

Die meisten Windows-Clients verhandeln standardmäßig die SMB-Signierung, sofern diese auf dem Server aktiviert ist. Wenn für einige Ihrer Windows-Clients SMB-Schutz erforderlich ist und die SMB-Signierung Leistungsprobleme verursacht, kann die SMB-Signierung auf allen Windows-Clients deaktiviert werden, die keinen Schutz vor Replay-Angriffen benötigen. Weitere Informationen zum Deaktivieren der SMB-Signierung auf Windows-Clients enthält die Microsoft Windows-Dokumentation.

ONTAP SMB Signaturkonfigurationsempfehlungen

Sie können das SMB-Signaturverhalten zwischen SMB-Clients und dem CIFS-Server an Ihre Sicherheitsanforderungen anpassen. Die Einstellungen, die bei der Konfiguration der SMB-Signatur auf dem CIFS-Server gewählt werden, hängen von den jeweiligen Sicherheitsanforderungen ab.

Sie können die SMB-Signatur entweder auf dem Client oder auf dem CIFS-Server konfigurieren. Bei der Konfiguration der SMB-Signatur sind die folgenden Empfehlungen zu berücksichtigen:

Wenn…	Empfehlung…
Die Sicherheit der Kommunikation zwischen Client und Server soll erhöht werden.	Die SMB-Signatur wird auf dem Client erforderlich gemacht, indem die `Require Option (Sign always)` Sicherheitseinstellung auf dem Client aktiviert wird.
Es wird gewünscht, dass der gesamte SMB-Datenverkehr zu einer bestimmten Storage Virtual Machine (SVM) signiert ist.	SMB-Signatur auf dem CIFS-Server erforderlich machen, indem die Sicherheitseinstellungen so konfiguriert werden, dass SMB-Signatur erforderlich ist.

Weitere Informationen zur Konfiguration der Windows Client-Sicherheitseinstellungen bietet die Microsoft-Dokumentation.

Informationen zur ONTAP SMB-Signaturkonfiguration für mehrere Daten-LIFS

Wenn Sie die erforderliche SMB-Signierung auf dem SMB-Server aktivieren oder deaktivieren, sollten die Richtlinien für mehrere Daten-LIFS-Konfigurationen für eine SVM bekannt sein.

Bei der Konfiguration eines SMB-Servers können mehrere Daten-LIFs eingerichtet sein. In diesem Fall enthält der DNS-Server mehrere `A` Einträge für den CIFS-Server, die alle denselben Hostnamen des SMB-Servers verwenden, aber jeweils eine eindeutige IP-Adresse besitzen. Beispielsweise könnte ein SMB-Server mit zwei konfigurierten Daten-LIFs die folgenden DNS `A` Einträge aufweisen:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Normalerweise werden bei einer Änderung der erforderlichen SMB-Signatur-Einstellung nur neue Verbindungen von Clients von der Änderung der SMB-Signatur-Einstellung betroffen. Es gibt jedoch eine Ausnahme von diesem Verhalten. Es gibt einen Fall, in dem ein Client bereits eine Verbindung zu einer

Freigabe hat und nach der Änderung der Einstellung eine neue Verbindung zur selben Freigabe herstellt, während die ursprüngliche Verbindung bestehen bleibt. In diesem Fall übernehmen sowohl die neue als auch die bestehende SMB-Verbindung die neuen SMB-Signatur-Anforderungen.

Das folgende Beispiel ist zu berücksichtigen:

1. Client1 stellt eine Verbindung zu einer Freigabe ohne erforderliche SMB-Signierung über den Pfad `O:\` her.
2. Der Speicheradministrator ändert die SMB-Server Konfiguration, sodass die SMB-Signierung erforderlich ist.
3. Client1 stellt eine Verbindung zur selben Freigabe mit der erforderlichen SMB-Signatur unter Verwendung des Pfads `S:\` (wobei die Verbindung unter Verwendung des Pfads `O:\` aufrechterhalten wird).
4. Das Ergebnis ist, dass die SMB-Signatur beim Zugriff auf Daten sowohl über das `O:\` als auch das `S:\` Laufwerk verwendet wird.

ONTAP-Signierung für eingehenden SMB-Datenverkehr konfigurieren

Sie können die Anforderung, dass Clients SMB-Nachrichten signieren, durch Aktivieren der erforderlichen SMB-Signierung durchsetzen. Wenn diese Option aktiviert ist, akzeptiert ONTAP SMB-Nachrichten nur, wenn sie gültige Signaturen aufweisen. Wenn die SMB-Signierung zugelassen, aber nicht vorgeschrieben werden soll, kann die erforderliche SMB-Signierung deaktiviert werden.

Über diese Aufgabe

Die erforderliche SMB-Signatur ist standardmäßig deaktiviert. Sie können die erforderliche SMB-Signatur jederzeit aktivieren oder deaktivieren.

> Die SMB-Signierung ist unter den folgenden Umständen nicht standardmäßig deaktiviert:
>
> 1. Die erforderliche SMB-Signierung ist aktiviert, und der Cluster wird auf eine Version von ONTAP zurückgesetzt, die die SMB-Signierung nicht unterstützt.
> 2. Anschließend erfolgt ein Upgrade des Clusters auf eine Version von ONTAP, die SMB-Signierung unterstützt.
>
>   Unter diesen Umständen bleibt die SMB-Signaturkonfiguration, die ursprünglich auf einer unterstützten Version von ONTAP konfiguriert wurde, auch bei einem Downgrade und einem anschließenden Upgrade erhalten.

Wenn eine Disaster-Recovery-Beziehung für eine Storage Virtual Machine (SVM) eingerichtet wird, bestimmt der Wert, der für die `-identity-preserve` Option des `snapmirror create` Befehls ausgewählt wird, welche Konfigurationsdetails in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, wird die SMB-Signatur-Sicherheitseinstellung auf das Ziel repliziert.

Wenn Sie die `-identity-preserve` Option auf `false` (non-ID-preserve) setzen, wird die SMB-Signatur-Sicherheitseinstellung nicht an das Ziel repliziert. In diesem Fall werden die CIFS-Server-Sicherheitseinstellungen auf dem Ziel auf die Standardwerte gesetzt. Wenn auf der Quell-SVM die erforderliche SMB-Signatur aktiviert ist, muss die erforderliche SMB-Signatur auf der Ziel-SVM manuell aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die erforderliche SMB-Signierung aktiviert werden soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -is-signing-required true`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -is-signing-required false`

2. Überprüfen Sie, ob die erforderliche SMB-Signierung aktiviert oder deaktiviert ist, indem festgestellt wird, ob der Wert im `Is Signing Required` Feld in der Ausgabe des folgenden Befehls auf den gewünschten Wert gesetzt ist: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Beispiel

Das folgende Beispiel aktiviert die erforderliche SMB-Signierung für SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

Änderungen an den Verschlüsselungseinstellungen werden für neue Verbindungen wirksam. Bestehende Verbindungen sind davon nicht betroffen.

Verwandte Informationen

- "snapmirror create"

Feststellen, ob ONTAP SMB-Sitzungen signiert sind

Informationen über verbundene SMB-Sitzungen auf dem CIFS-Server können angezeigt werden. Diese Informationen ermöglichen die Feststellung, ob SMB-Sitzungen signiert sind. Dies kann hilfreich sein, um zu bestimmen, ob SMB-Client-Sitzungen mit den gewünschten Sicherheitseinstellungen verbunden sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
Alle signierten Sitzungen auf einer bestimmten Storage Virtual Machine (SVM)	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Details zu einer signierten Sitzung mit einer bestimmten Sitzungs-ID auf der SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Beispiele

Der folgende Befehl zeigt Sitzungsinformationen zu signierten Sitzungen auf SVM vs1 an. Die Standard-Zusammenfassungsausgabe zeigt das Ausgabefeld „`Ist Sitzung signiert`“ nicht an:

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

Der folgende Befehl zeigt detaillierte Sitzungsinformationen an, einschließlich der Information, ob die Sitzung signiert ist, für eine SMB-Sitzung mit der Sitzungs-ID 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Verwandte Informationen

Überwachung von SMB-signierten Sitzungsstatistiken

ONTAP SMB-signierte Sitzungsstatistiken überwachen

Sie können SMB-Sitzungsstatistiken überwachen und feststellen, welche bestehenden Sitzungen signiert sind und welche nicht.

Über diese Aufgabe

Der `statistics`Befehl auf der erweiterten Berechtigungsstufe stellt den `signed_sessions`Zähler bereit, mit dem die Anzahl der signierten SMB-Sitzungen überwacht werden kann. Der `signed_sessions`Zähler ist mit den folgenden Statistiken-Objekten verfügbar:

- `cifs`ermöglicht die Überwachung der SMB-Signierung für alle SMB-Sitzungen.
- `smb1` Ermöglicht die Überwachung der SMB-Signatur für SMB 1.0-Sitzungen.
- `smb2`ermöglicht die Überwachung der SMB-Signierung für SMB 2.x und SMB 3.0 Sitzungen.

  Die SMB 3.0 Statistiken sind in der Ausgabe für das `smb2` Objekt enthalten.

Wenn Sie die Anzahl der signierten Sitzungen mit der Gesamtzahl der Sitzungen vergleichen möchten, kann die Ausgabe für den `signed_sessions` Counter mit der Ausgabe für den `established_sessions` Counter verglichen werden.

Sie müssen eine Statistiken Stichprobenerfassung starten, bevor Sie die resultierenden Daten anzeigen können. Daten aus der Stichprobe können angezeigt werden, wenn die Datenerfassung nicht gestoppt wird. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird, besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Trends zu erkennen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
   `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn der `-sample-id` Parameter nicht angegeben wird, generiert der Befehl eine Beispielkennung für Sie und definiert dieses Beispiel als das Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` ist ein Text-String. Wenn dieser Befehl während derselben CLI-Sitzung ausgeführt wird und der `-sample -id` Parameter nicht angegeben wird, überschreibt der Befehl das vorherige Standardbeispiel.

   Sie können optional den Knoten angeben, auf dem Sie Statistiken erfassen möchten. Wenn Sie keinen Knoten angeben, erfasst das Beispiel Statistiken für alle Knoten im Cluster.

   Weitere Informationen zu `statistics start` finden sich in der "ONTAP-Befehlsreferenz".
3. Mit dem `statistics stop` Befehl wird das Sammeln von Daten für die Probe gestoppt.

   Weitere Informationen zu `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".
4. SMB-Signaturstatistiken anzeigen:

Wenn Sie Informationen zu … anzeigen möchten	Eingeben…
Unterzeichnete Sitzungen	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Signierte Sitzungen und etablierte Sitzungen
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

Wenn Informationen nur für einen einzelnen Knoten angezeigt werden sollen, kann der optionale `-node`Parameter angegeben werden.

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

5. Zurück zur Administratorrechteebene:
`set -privilege admin`

▼ **Beispiele**

Das folgende Beispiel zeigt, wie die Signaturstatistiken von SMB 2.x und SMB 3.0 auf der Storage Virtual Machine (SVM) vs1 überwacht werden können.

Der folgende Befehl wechselt zur erweiterten Berechtigungsstufe:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

Der folgende Befehl beendet die Datenerfassung für das Beispiel:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

Der folgende Befehl zeigt signierte SMB-Sitzungen und aufgebaute SMB-Sitzungen pro Knoten aus dem Beispiel:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name
```

```
Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                 Value
    -------------------------------- -------------------------
    established_sessions                                        0
    node_name                                               node1
    signed_sessions                                             0
    established_sessions                                        1
    node_name                                               node2
    signed_sessions                                             1
    established_sessions                                        0
    node_name                                               node3
    signed_sessions                                             0
    established_sessions                                        0
    node_name                                               node4
    signed_sessions                                             0
```

Der folgende Befehl zeigt signierte SMB-Sitzungen für node2 aus dem Beispiel an:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                 Value
    -------------------------------- -------------------------
    node_name                                               node2
    signed_sessions                                             1
```

Der folgende Befehl wechselt zurück auf die Administratorrechteebene:

```
cluster1::*> set -privilege admin
```

Verwandte Informationen

- Feststellen, ob SMB-Sitzungen signiert sind
- "Überblick über Leistungsüberwachung und Management"

Erforderliche SMB-Verschlüsselung auf SMB-Servern für Datenübertragungen über SMB konfigurieren

Informationen zur ONTAP SMB-Verschlüsselung

Die SMB-Verschlüsselung für Datenübertragungen über SMB ist eine Sicherheitsverbesserung, die auf SMB-Servern aktiviert oder deaktiviert werden kann. Die gewünschte SMB-Verschlüsselungseinstellung kann auch für jede einzelne Freigabe über eine Freigabeeigenschaft konfiguriert werden.

Standardmäßig ist die SMB-Verschlüsselung deaktiviert, wenn ein SMB-Server auf der Storage Virtual Machine (SVM) erstellt wird. Sie muss aktiviert werden, um von der erhöhten Sicherheit durch die SMB-Verschlüsselung zu profitieren.

Um eine verschlüsselte SMB-Sitzung zu erstellen, muss der SMB-Client die SMB-Verschlüsselung unterstützen. Windows Clients ab Windows Server 2012 und Windows 8 unterstützen die SMB-Verschlüsselung.

Die SMB-Verschlüsselung auf der SVM wird durch zwei Einstellungen gesteuert:

- Eine SMB-Server-Sicherheitsoption, die die Funktionalität auf der SVM ermöglicht
- Eine SMB-Freigabeeigenschaft, die die SMB-Verschlüsselungseinstellung für jede einzelne Freigabe konfiguriert

Sie können entscheiden, ob für den Zugriff auf alle Daten auf der SVM eine Verschlüsselung erforderlich sein soll oder ob für den Zugriff auf Daten nur in ausgewählten Freigaben SMB-Verschlüsselung erforderlich sein soll. Die `encrypt-data` Freigabeeigenschaft erfordert SMB-Verschlüsselung für den Zugriff auf eine Freigabe. Ab ONTAP 9.11.1 ermöglicht die `allow-unencrypted-access` Freigabeeigenschaft SMB2-Clients den Zugriff auf eine Freigabe ohne Verschlüsselung, während SMB3-Clients weiterhin Verschlüsselung verwenden, wenn `encrypt-data` aktiviert ist.

SVM-Einstellungen haben Vorrang vor Freigabeeinstellungen.

Die effektive SMB-Verschlüsselungskonfiguration hängt von der Kombination der beiden Einstellungen ab und ist in der folgenden Tabelle beschrieben:

SMB-Server mit aktivierter SMB-Verschlüsselung	Einstellung „Daten verschlüsseln“ für die Freigabe aktiviert	Einstellung „Unverschlüsselten Zugriff zulassen“ aktiviert	Server-seitiges Verschlüsselungsverhalten
True	Falsch	Falsch	Die serverseitige Verschlüsselung ist für alle Freigaben in der SVM aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.

SMB-Server mit aktivierter SMB-Verschlüsselung	Einstellung „Daten verschlüsseln“ für die Freigabe aktiviert	Einstellung „Unverschlüsselten Zugriff zulassen“ aktiviert	Server-seitiges Verschlüsselungsverhalten
True	True	Falsch	Die serverseitige Verschlüsselung ist für alle Freigaben in der SVM aktiviert, unabhängig von der Freigabeverschlüsselung. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.
Falsch	True	Falsch	Die Freigabeverschlüsselung ist für die betreffenden Freigaben aktiviert. SMB3 Clients verwenden Verschlüsselung, SMB2 Clients können jedoch unverschlüsselt auf die Freigabe zugreifen, da die `allow-unencrypted-access`Eigenschaft aktiviert ist.
Falsch	Falsch	Falsch	Es ist keine Verschlüsselung aktiviert.
Falsch	Falsch	True	Es ist keine Verschlüsselung aktiviert. Die `allow-unencrypted-access` Eigenschaft hat keine Auswirkung, sofern `encrypt-data` nicht aktiviert ist.

SMB-Clients, die keine Verschlüsselung unterstützen, können keine Verbindung zu einem SMB-Server oder einer Freigabe herstellen, die eine Verschlüsselung erfordert.

Änderungen an den Verschlüsselungseinstellungen werden für neue Verbindungen wirksam. Bestehende Verbindungen sind davon nicht betroffen.

Die `allow-unencrypted-access` Eigenschaft wird ab ONTAP 9.11.1 unterstützt.

Die SMB-Verschlüsselung auf SVM-Ebene überschreibt die Einstellungen auf Freigabeebene.

Informationen zu den Auswirkungen der ONTAP SMB-Verschlüsselung auf die Performance

Wenn SMB-Sitzungen SMB-Verschlüsselung verwenden, kommt es bei der gesamten

SMB-Kommunikation mit Windows-Clients zu Leistungseinbußen, die sowohl die Clients als auch den Server betreffen (das heißt, die Knoten im Cluster, auf denen die SVM ausgeführt wird, die den SMB-Server enthält).

Die Auswirkungen auf die Leistung zeigen sich in einer erhöhten CPU-Auslastung sowohl auf den Clients als auch auf dem Server, obwohl sich das Netzwerkverkehr nicht ändert.

Das Ausmaß der Leistungseinbußen hängt von der Version von ONTAP 9 ab, die Sie verwenden. Ab ONTAP 9.7 kann ein neuer Verschlüsselungs-Offload-Algorithmus eine bessere Performance im verschlüsselten SMB-Datenverkehr ermöglichen. Die SMB-Verschlüsselungsauslagerung ist standardmäßig aktiviert, wenn die SMB-Verschlüsselung aktiviert ist.

Für eine verbesserte SMB-Verschlüsselungsleistung ist die AES-NI-Offload-Funktion erforderlich. Im Hardware Universe (HWU) kann überprüft werden, ob für Ihre Plattform AES-NI-Offload unterstützt wird.

Weitere Leistungsverbesserungen sind ebenfalls möglich, wenn Sie SMB Version 3.11 verwenden können, die den wesentlich schnelleren GCM Algorithmus unterstützt.

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung kann der Einfluss der SMB-Verschlüsselung auf die Leistung stark variieren; dies lässt sich nur durch Tests in Ihrer Netzwerkumgebung überprüfen.

Die SMB-Verschlüsselung ist auf dem SMB-Server standardmäßig deaktiviert. Die SMB-Verschlüsselung sollte nur für diejenigen SMB-Freigaben oder SMB-Server aktiviert werden, die eine Verschlüsselung benötigen. Mit SMB-Verschlüsselung führt ONTAP für jede Anfrage eine zusätzliche Verarbeitung durch, indem die Anfragen entschlüsselt und die Antworten verschlüsselt werden. Die SMB-Verschlüsselung sollte daher nur bei Bedarf aktiviert werden.

ONTAP SMB-Verschlüsselung für eingehenden Datenverkehr aktivieren oder deaktivieren

Wenn die SMB-Verschlüsselung für eingehenden SMB-Datenverkehr erforderlich sein soll, kann sie auf dem CIFS-Server oder auf Freigabeebene aktiviert werden. Standardmäßig ist die SMB-Verschlüsselung nicht erforderlich.

Über diese Aufgabe

Sie können die SMB-Verschlüsselung auf dem CIFS-Server aktivieren, wodurch sie für alle Freigaben auf dem CIFS-Server gilt. Wenn für alle Freigaben auf dem CIFS-Server keine verpflichtende SMB-Verschlüsselung erforderlich sein soll oder wenn verpflichtende SMB-Verschlüsselung für eingehenden SMB-Datenverkehr nur für einzelne Freigaben aktiviert werden soll, kann die verpflichtende SMB-Verschlüsselung auf dem CIFS-Server deaktiviert werden.

Wenn Sie eine Storage Virtual Machine (SVM) Notfallwiederherstellungsbeziehung einrichten, bestimmt der Wert, den Sie für die `-identity-preserve` Option des `snapmirror create` Befehls auswählen, die Konfigurationsdetails, die in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, wird die SMB-Verschlüsselungssicherheitseinstellung auf das Ziel repliziert.

Wenn die `-identity-preserve` Option auf `false` (non-ID-preserve) gesetzt ist, wird die SMB-Verschlüsselungssicherheitseinstellung nicht auf das Ziel repliziert. In diesem Fall werden die CIFS-Server-Sicherheitseinstellungen auf dem Ziel auf die Standardwerte gesetzt. Wenn auf der Quell-SVM die SMB-Verschlüsselung aktiviert ist, muss die CIFS-Server-SMB-Verschlüsselung auf dem Ziel manuell aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr auf dem CIFS-Server benötigt wird…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false`

2. Es sollte überprüft werden, ob die erforderliche SMB-Verschlüsselung auf dem CIFS-Server wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

   Das `is-smb-encryption-required` Feld zeigt `true` an, wenn die erforderliche SMB-Verschlüsselung auf dem CIFS-Server aktiviert ist, und `false` wenn sie deaktiviert ist.

Beispiel

Das folgende Beispiel aktiviert die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr für den CIFS-Server auf SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Verwandte Informationen

- "snapmirror create"

Ermitteln, ob Clients über verschlüsselte ONTAP SMB-Sitzungen verbunden sind.

Sie können Informationen über verbundene SMB-Sitzungen anzeigen, um festzustellen, ob Clients verschlüsselte SMB-Verbindungen verwenden. Dies kann hilfreich sein, um zu bestimmen, ob SMB-Client-Sitzungen mit den gewünschten Sicherheitseinstellungen verbunden sind.

Über diese Aufgabe

Die Sitzungen von SMB-Clients können eine von drei Verschlüsselungsstufen aufweisen:

- `unencrypted`

Die SMB-Sitzung ist nicht verschlüsselt. Weder auf Storage Virtual Machine (SVM)-Ebene noch auf Freigabeebene ist eine Verschlüsselung konfiguriert.

- `partially-encrypted`

  Die Verschlüsselung wird beim Tree-Connect initiiert. Die Verschlüsselung auf Freigabeebene ist konfiguriert. Die Verschlüsselung auf SVM-Ebene ist nicht aktiviert.

- `encrypted`

  Die SMB-Sitzung ist vollständig verschlüsselt. Die SVM-Verschlüsselung ist aktiviert. Die Freigabeverschlüsselung kann aktiviert sein oder nicht. Die Einstellung für die SVM-Verschlüsselung hat Vorrang vor der Einstellung für die Freigabeverschlüsselung.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
Sitzungen mit einer festgelegten Verschlüsselungseinstellung für Sitzungen auf einer bestimmten SVM	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
Die Verschlüsselungseinstellung für eine bestimmte Sitzungs-ID auf einer bestimmten SVM	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

Beispiele

Der folgende Befehl zeigt detaillierte Sitzungsinformationen, einschließlich der Verschlüsselungseinstellung, zu einer SMB-Sitzung mit der Sitzungs-ID 2 an:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
```

```
            Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

ONTAP SMB-Verschlüsselungsstatistiken überwachen

Sie können die SMB-Verschlüsselungsstatistiken überwachen und feststellen, welche hergestellten Sitzungen und Freigabeverbindungen verschlüsselt sind und welche nicht.

Über diese Aufgabe

Der `statistics` Befehl auf der Ebene mit erweiterten Berechtigungen stellt die folgenden Zähler bereit, mit denen Sie die Anzahl der verschlüsselten SMB-Sitzungen und Freigabeverbindungen überwachen können:

Zählername	Beschreibungen
`encrypted_sessions`	Gibt die Anzahl der verschlüsselten SMB 3.0 Sitzungen an.
`encrypted_share_connections`	Gibt die Anzahl der verschlüsselten Anteile an, auf denen eine Baumverbindung stattgefunden hat
`rejected_unencrypted_sessions`	Gibt die Anzahl der abgelehnten Sitzungsaufbauten aufgrund fehlender Client-Verschlüsselungsfunktionen an
`rejected_unencrypted_shares`	Gibt die Anzahl der aufgrund fehlender Client-Verschlüsselungsfunktionen abgelehnten Freigabezuordnungen an

Diese Zähler sind mit den folgenden Statistiken-Objekten verfügbar:

- `cifs`ermöglicht die Überwachung der SMB-Verschlüsselung für alle SMB 3.0-Sitzungen.

  Die SMB 3.0 Statistiken sind in der Ausgabe für das `cifs` Objekt enthalten. Wenn die Anzahl der verschlüsselten Sitzungen mit der Gesamtzahl der Sitzungen verglichen werden soll, kann die Ausgabe für den `encrypted_sessions` Counter mit der Ausgabe für den `established_sessions` Counter verglichen werden.

  Wenn Sie die Anzahl der verschlüsselten Freigabeverbindungen mit der Gesamtzahl der Freigabeverbindungen vergleichen möchten, kann die Ausgabe für den `encrypted_share_connections` Counter mit der Ausgabe für den `connected_shares` Counter verglichen werden.

- `rejected_unencrypted_sessions`Gibt die Anzahl der Versuche an, eine SMB-Sitzung herzustellen, die eine Verschlüsselung erfordert, von einem Client, der SMB-Verschlüsselung nicht unterstützt.
- `rejected_unencrypted_shares`Gibt die Anzahl der Versuche an, eine Verbindung zu einer SMB-Freigabe herzustellen, die eine Verschlüsselung erfordert, von einem Client, der SMB-Verschlüsselung nicht unterstützt.

Sie müssen eine Statistiken Stichprobenerfassung starten, bevor Sie die resultierenden Daten anzeigen können. Sie können Daten aus der Stichprobe anzeigen, wenn Sie die Datenerfassung nicht beenden. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird,

besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Trends zu erkennen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
   `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   Wenn der `-sample-id` Parameter nicht angegeben wird, generiert der Befehl eine Beispielkennung für Sie und definiert dieses Beispiel als das Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` ist ein Text-String. Wenn dieser Befehl während derselben CLI-Sitzung ausgeführt wird und der `-sample-id` Parameter nicht angegeben wird, überschreibt der Befehl das vorherige Standardbeispiel.

   Sie können optional den Knoten angeben, auf dem Sie Statistiken erfassen möchten. Wenn Sie keinen Knoten angeben, erfasst das Beispiel Statistiken für alle Knoten im Cluster.

   Weitere Informationen zu `statistics start` finden sich in der "ONTAP-Befehlsreferenz".
3. Mit dem `statistics stop` Befehl wird das Sammeln von Daten für die Probe gestoppt.

   Weitere Informationen zu `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".
4. SMB-Verschlüsselungsstatistiken:

Wenn Sie Informationen zu … anzeigen möchten	Eingeben…
Verschlüsselte Sitzungen	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Verschlüsselte Sitzungen und etablierte Sitzungen
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Verschlüsselte Freigabeverbindungen
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Verschlüsselte Freigabeverbindungen und verbundene Freigaben	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Abgelehnte unverschlüsselte Sitzungen	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Abgelehnte unverschlüsselte Freigabeverbindungen
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

   Wenn Informationen nur für einen einzelnen Knoten angezeigt werden sollen, kann der optionale `-node`Parameter angegeben werden.

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

5. Zurück zur Administratorrechteebene:
`set -privilege admin`

▼ **Beispiele**

Das folgende Beispiel zeigt, wie die SMB 3.0 Verschlüsselungsstatistiken auf einer Storage Virtual Machine (SVM) vs1 überwacht werden können.

Der folgende Befehl wechselt zur erweiterten Berechtigungsstufe:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

Der folgende Befehl beendet die Datenerfassung für diese Stichprobe:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

Der folgende Befehl zeigt verschlüsselte SMB-Sitzungen und aufgebaute SMB-Sitzungen des Knotens aus dem Beispiel an:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
```

```
    established_sessions                    1
    encrypted_sessions                      1

2 entries were displayed
```

Der folgende Befehl zeigt die Anzahl der vom Knoten aus dem Beispiel abgelehnten unverschlüsselten SMB-Sitzungen an:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    rejected_unencrypted_sessions                1

1 entry was displayed.
```

Der folgende Befehl zeigt die Anzahl der verbundenen SMB-Freigaben und der verschlüsselten SMB-Freigaben nach dem Knoten aus dem Beispiel:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                             2
    encrypted_share_connections                  1

2 entries were displayed.
```

Der folgende Befehl zeigt die Anzahl der vom Knoten aus dem Beispiel abgelehnten unverschlüsselten SMB-Freigabeverbindungen:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                    1

1 entry was displayed.
```

Verwandte Informationen

- Welche Statistiken, Objekte und Zähler auf den Servern verfügbar sind, lässt sich feststellen.
- "Überblick über Leistungsüberwachung und Management"

Sichere LDAP-Sitzungskommunikation

Informationen zu ONTAP SMB LDAP-Signierung und -Versiegelung

Ab ONTAP 9 können Sie die Signierung und Versiegelung konfigurieren, um die LDAP-Sitzungssicherheit bei Abfragen an einen Active Directory (AD)-Server zu aktivieren. Die CIFS-Server-Sicherheitseinstellungen auf der Storage Virtual Machine (SVM) müssen so konfiguriert werden, dass sie mit denen des LDAP-Servers übereinstimmen.

Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe einer geheimen Schlüsseltechnologie. Versiegeln verschlüsselt die LDAP-Nutzlastdaten, um die Übertragung sensibler Informationen im Klartext zu vermeiden. Eine Option für den *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt oder keines von beidem sein muss. Der Standardwert ist `none`.

Die LDAP-Signierung und -Versiegelung des CIFS-Datenverkehrs ist auf der SVM mit der `-session -security-for-ad-ldap` Option zum `vserver cifs security modify` Befehl aktiviert.

LDAP-Signierung und -Versiegelung auf ONTAP SMB-Servern aktivieren

Bevor Ihr CIFS-Server die Signierung und Versiegelung für die sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, sind die Sicherheitseinstellungen des CIFS-Servers so zu ändern, dass LDAP-Signierung und -Versiegelung aktiviert werden.

Bevor Sie beginnen

Es ist erforderlich, sich mit Ihrem AD-Serveradministrator abzustimmen, um die geeigneten Sicherheitskonfigurationswerte zu ermitteln.

Schritte

1. Die CIFS-Server-Sicherheitseinstellung konfigurieren, die signierten und versiegelten Datenverkehr mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver vserver_name -session-security-for-ad-ldap {none|sign|seal}`

   Sie können Signieren (`sign`, Datenintegrität, Signieren und Versiegeln (`seal`, Datenintegrität und Verschlüsselung oder keines von beidem `none`, keine Signierung oder Versiegelung, aktivieren. Der Standardwert ist `none`.

2. Überprüfen, ob die LDAP-Signatur- und Versiegelungssicherheitseinstellung korrekt konfiguriert ist: `vserver cifs security show -vserver vserver_name`

> Wenn die SVM denselben LDAP-Server für die Abfrage von Namenszuordnungen oder anderen UNIX-Informationen wie Benutzern, Gruppen und Netzgruppen verwendet, muss die entsprechende Einstellung mit der `-session-security` Option des `vserver services name-service ldap client modify` Befehls aktiviert werden.

LDAP über TLS für ONTAP SMB-Server konfigurieren

Konfigurieren Sie LDAP über TLS für ONTAP SMB-Server, um die Kommunikation zwischen dem SMB-Server und Active Directory LDAP-Servern zu sichern.

Schritt 1: Selbstsignierte Stammzertifizierungsstellenzertifikate für ONTAP SMB SVMs exportieren

Um LDAP über SSL/TLS zur Sicherung der Active Directory-Kommunikation zu verwenden, muss zunächst eine Kopie des selbstsignierten Stammzertifikats des Active Directory Certificate Service in eine Zertifikatsdatei exportiert und in eine ASCII-Textdatei konvertiert werden. Diese Textdatei wird von ONTAP verwendet, um das Zertifikat auf der Storage Virtual Machine (SVM) zu installieren.

Der Active Directory-Zertifikatdienst muss für die Domäne, zu der der CIFS-Server gehört, bereits installiert und konfiguriert sein. Informationen zur Installation und Konfiguration von Active Directory Certificate Services finden Sie in der Dokumentation "Microsoft TechNet Bibliothek: technet.microsoft.com"

> Ab ONTAP 9.13.1 ist, wenn `-use-start-tls-for-ad-ldap` oder `-use-ldaps-for-ad-ldap` für den SMB-Server aktiviert ist, sicherzustellen, dass die erforderlichen CA-Zertifikate für vertrauenswürdige Domänen sowie für die Heimatdomäne installiert sind. ONTAP muss TLS- oder LDAPS-Verbindungen zu Domänencontrollern vertrauenswürdiger Domänen herstellen können, um deren Standortinformationen zu ermitteln.

Schritt

1. Ein Root-CA-Zertifikat des Domänencontrollers im `.pem` Textformat erhalten.

   "Microsoft TechNet Bibliothek: technet.microsoft.com"

Was kommt als Nächstes

Das Zertifikat auf der SVM installieren.

Schritt 2: Installieren Sie selbstsignierte Stammzertifikate der Zertifizierungsstelle auf der ONTAP SMB SVM

Wenn bei der Anbindung an LDAP-Server eine LDAP-Authentifizierung mit TLS erforderlich ist, muss zunächst das selbstsignierte Root-CA-Zertifikat auf der SVM installiert werden.

Über diese Aufgabe

Alle Anwendungen innerhalb von ONTAP, die TLS-Kommunikation nutzen, können den Status digitaler Zertifikate mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Wenn OCSP für LDAP über TLS aktiviert ist, werden widerrufene Zertifikate zurückgewiesen und die Verbindung schlägt fehl.

Schritte

1. Das selbstsignierte Stammzertifikat der Zertifizierungsstelle installieren:
   a. Beginnen Sie die Zertifikatsinstallation:

      ```
      security certificate install -vserver <SVM_name> -type server-ca
      ```

      Die Konsolenausgabe zeigt folgende Meldung an: `Please enter Certificate: Press <Enter> when done`

   b. Öffnen Sie die `.pem` Zertifikatsdatei mit einem Texteditor, das Zertifikat einschließlich der Zeilen kopieren, die mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----` enden, und das Zertifikat anschließend nach der Eingabeaufforderung einfügen.
   c. Es wird überprüft, ob das Zertifikat korrekt angezeigt wird.
   d. Die Installation wird durch Drücken der Eingabetaste abgeschlossen.
2. Überprüfen Sie, ob das Zertifikat installiert ist:

   ```
   security certificate show -vserver <SVM_name>
   ```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"

Schritt 3: LDAP über TLS auf dem ONTAP SMB-Server aktivieren

Bevor Ihr SMB-Server TLS für die sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen die Sicherheitseinstellungen des SMB-Servers geändert werden, damit LDAP über TLS genutzt werden kann.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory (AD) als auch für Namensdienst-LDAP-Verbindungen unterstützt. ONTAP versucht die Kanalbindung mit LDAP-Verbindungen nur, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Versiegeln eingestellt ist. Um die LDAP-Kanalbindung mit AD-Servern zu deaktivieren oder wieder zu aktivieren, kann der `-try-channel-binding-for-ad-ldap` Parameter mit dem `vserver cifs security modify` Befehl verwendet werden.

Weitere Informationen sind unter folgendem Link verfügbar:

- "Informationen zu LDAP für ONTAP NFS SVMs"
- "LDAP-Kanalbindungs- und LDAP-Signaturanforderungen für Windows 2020".

Schritte

1. Konfigurieren Sie die SMB-Server-Sicherheitseinstellung, die eine sichere LDAP-Kommunikation mit Active

Directory LDAP-Servern ermöglicht:

```
vserver cifs security modify -vserver <SVM_name> -use-start-tls-for-ad
-ldap true
```

Ab ONTAP 9.13.1 verwendet ONTAP, wenn die sichere LDAP-Kommunikation für Active Directory-Verbindungen aktiviert ist, diese sicheren Verbindungen auch für die Kontaktaufnahme mit Domänencontrollern vertrauenswürdiger Domänen. Wenn die erforderlichen Zertifikate für Domänencontroller vertrauenswürdiger Domänen nicht installiert sind, kann ONTAP möglicherweise keine Standortinformationen zu vertrauenswürdigen Domänen ermitteln.

2. Überprüfen Sie, ob die LDAP-über-TLS-Sicherheitseinstellung auf `true` gesetzt ist:

```
vserver cifs security show -vserver <SVM_name>
```

Wenn die SVM denselben LDAP-Server für die Abfrage von Namenszuordnungen oder anderen UNIX-Informationen (wie Benutzern, Gruppen und Netzgruppen) verwendet, muss auch die Option `-use-start-tls` mit dem Befehl `vserver services name-service ldap client modify` geändert werden.

Dateizugriff mit SMB einrichten

Sicherheitsstile konfigurieren

Informationen zu ONTAP SMB-Sicherheitsstilen und deren Auswirkungen

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

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

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

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Resultierender effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Unix	NFS	• NFSv3 Modusbits • NFSv4.x-ACLs	Unix	NFS und SMB

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

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

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

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

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

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

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

Zur Unterstützung bei der Entscheidung, welchen Sicherheitsstil Sie für ein Volume verwenden, sind zwei

Faktoren zu berücksichtigen. Der wichtigste Faktor ist die Art des Administrators, der das Dateisystem verwaltet. Der zweite Faktor ist die Art des Benutzers oder Dienstes, der auf die Daten auf dem Volume zugreift.

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

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

Informationen zur Vererbung des Sicherheitsstils bei ONTAP SMB

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

Sicherheitsstile werden folgendermaßen vererbt:

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

SMB-Sicherheitsstile auf ONTAP SVM Root-Volumes konfigurieren

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

Schritte

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

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

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

SMB-Sicherheitsstile auf ONTAP FlexVol Volumes konfigurieren

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

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

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

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

SMB-Sicherheitsstile auf ONTAP Qtrees konfigurieren

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

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

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

Daten-Volumes in NAS-Namespaces erstellen und verwalten

Informationen zum Erstellen und Verwalten von ONTAP SMB-Datenvolumes in NAS-Namespaces

Um den Dateizugriff in einer NAS-Umgebung zu verwalten, müssen Sie Datenvolumes und Verbindungspunkte auf Ihrer Storage Virtual Machine (SVM) verwalten. Dies umfasst die Planung Ihrer Namespace-Architektur, das Erstellen von Volumes mit oder ohne Verbindungspunkte, das Einbinden oder Aushängen von Volumes sowie das Anzeigen von Informationen über Datenvolumes und NFS-Server- oder CIFS-Server-Namespaces.

ONTAP SMB-Datenvolumes mit angegebenen Verbindungspunkten erstellen

Beim Erstellen eines Datenvolumes kann der Verbindungspunkt festgelegt werden. Das resultierende Volume wird automatisch am Verbindungspunkt eingebunden und steht sofort zur Konfiguration für den NAS-Zugriff bereit.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.

> Folgende Zeichen dürfen im Verbindungspfad nicht verwendet werden: * # " > < | ? \
>
> Darüber hinaus darf die Verbindungspfadlänge nicht mehr als 255 Zeichen betragen.

Schritte

1. Das Volume mit einer Verbindung erstellen: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

   Der Verbindungspfad muss mit dem Stammverzeichnis (/) beginnen und kann sowohl Verzeichnisse als auch verknüpfte Volumes enthalten. Der Verbindungspfad muss nicht den Namen des Volumes enthalten. Verbindungspfade sind unabhängig vom Volume-Namen.

   Die Angabe eines Sicherheitsstils für das Volume ist optional. Wenn kein Sicherheitsstil angegeben wird, erstellt ONTAP das Volume mit demselben Sicherheitsstil, der auf das Root-Volume der Storage Virtual Machine (SVM) angewendet wird. Der Sicherheitsstil des Root-Volumes entspricht jedoch möglicherweise nicht dem Sicherheitsstil, der für das zu erstellende Datenvolume gewünscht ist. Es empfiehlt sich, den Sicherheitsstil beim Erstellen des Volumes anzugeben, um schwer zu behebende Probleme beim Dateizugriff zu minimieren.

   Der Verbindungspfad ist nicht Groß-/Kleinschreibung-abhängig; `/ENG` ist identisch mit `/eng`. Wird eine CIFS-Freigabe erstellt, behandelt Windows den Verbindungspfad so, als ob er Groß-/Kleinschreibung-abhängig ist. Beispielsweise muss, wenn die Verbindung `/ENG` ist, der Pfad einer CIFS-Freigabe mit `/ENG` beginnen und nicht mit `/eng`.

   Es gibt zahlreiche optionale Parameter, mit denen Sie ein Datenvolumen anpassen können. Weitere

Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob das Volume mit dem gewünschten Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Das folgende Beispiel erstellt ein Volume namens “home4” auf SVM vs1, das einen Verbindungspfad hat `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

ONTAP SMB-Datenvolumes ohne Angabe von Verbindungspunkten erstellen

Sie können ein Datenvolume erstellen, ohne einen Verbindungspunkt anzugeben. Das resultierende Volume wird nicht automatisch eingebunden und steht nicht zur Konfiguration für NAS-Zugriff zur Verfügung. Das Volume muss eingebunden werden, bevor SMB-Freigaben oder NFS-Exporte für dieses Volume konfiguriert werden können.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.

Schritte

1. Das Volume ohne Verbindungspunkt kann mit folgendem Befehl erstellt werden: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Die Angabe eines Sicherheitsstils für das Volume ist optional. Wenn kein Sicherheitsstil angegeben wird, erstellt ONTAP das Volume mit demselben Sicherheitsstil, der auf das Root-Volume der Storage Virtual Machine (SVM) angewendet wird. Der Sicherheitsstil des Root-Volumes entspricht jedoch möglicherweise nicht dem gewünschten Sicherheitsstil für das Datenvolume. Es empfiehlt sich, den Sicherheitsstil beim Erstellen des Volumes anzugeben, um schwer zu behebende Probleme beim Dateizugriff zu minimieren.

   Es gibt zahlreiche optionale Parameter, mit denen Sie ein Datenvolumen anpassen können. Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Es wird überprüft, ob das Volume ohne Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Das folgende Beispiel erstellt ein Volume mit dem Namen “sales”, das sich auf SVM vs1 befindet und nicht an einem Verbindungspunkt eingebunden ist:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

Vorhandene ONTAP SMB-Volumes im NAS-Namespace einbinden oder aushängen

Ein Volume muss im NAS-Namespace eingebunden sein, bevor Sie den NAS-Client-Zugriff auf die in den Storage Virtual Machine (SVM)-Volumes enthaltenen Daten konfigurieren können. Ein Volume kann an einem Verbindungspunkt eingebunden werden, wenn es derzeit nicht eingebunden ist. Volumes können auch ausgehängt werden.

Über diese Aufgabe

Wenn ein Volume ausgehängt und offline genommen wird, sind alle Daten innerhalb der Verbindung, einschließlich der Daten in Volumes mit Verbindungen innerhalb des Namespace des ausgehängten Volumes, für NAS-Clients nicht zugänglich.

> Um den Dateizugriff eines NAS-Clients auf ein Volume zu beenden, reicht es nicht aus, das Volume einfach auszuhängen. Das Volume muss offline genommen werden oder es sind andere Maßnahmen erforderlich, um sicherzustellen, dass Client-seitig Dateihandle-Caches ungültig werden. Weitere Informationen enthält der folgende Knowledge Base Artikel: "NFSv3-Clients haben weiterhin Zugriff auf ein Volume, nachdem sie aus dem Namespace in ONTAP entfernt wurden"

Wenn ein Volume ausgehängt und offline genommen wird, gehen die darin enthaltenen Daten nicht verloren. Zudem bleiben bestehende Volume-Exportrichtlinien und SMB-Shares, die auf dem Volume oder in Verzeichnissen und Verbindungspunkten innerhalb des ausgehängten Volumes erstellt wurden, erhalten. Wird das ausgehängte Volume wieder eingebunden, können NAS-Clients mit den bestehenden Exportrichtlinien und SMB-Shares auf die darin enthaltenen Daten zugreifen.

Schritte

1. Die gewünschte Aktion ausführen:

Wenn Sie möchten…	Die Befehle werden eingegeben…
Ein Volume einbinden	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Wenn Sie möchten…	Die Befehle werden eingegeben…

Aushängen eines Volumes	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Es sollte sichergestellt werden, dass sich das Volume im gewünschten Mount-Status befindet:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Beispiele

Das folgende Beispiel bindet ein Volume namens “sales”, das sich auf SVM “vs1” befindet, an den Verbindungspunkt “/sales” ein:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Das folgende Beispiel hängt ein Volume namens “data” auf SVM “vs1” aus und nimmt es offline:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Informationen zu ONTAP SMB-Volume-Mounts und Verbindungspunkten anzeigen

Sie können Informationen zu eingebundenen Volumes für Storage Virtual Machines (SVMs) und den Verbindungspunkten, an die die Volumes eingebunden sind, anzeigen. Es lässt sich auch feststellen, welche Volumes nicht an einen Verbindungspunkt

eingebunden sind. Diese Informationen ermöglichen ein besseres Verständnis und eine effektivere Verwaltung Ihres SVM-Namespaces.

Schritte

1. Die gewünschte Aktion ausführen:

Wenn Sie anzeigen möchten…	Geben Sie den Befehl ein…
Zusammenfassende Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	`volume show -vserver vserver_name -junction`
Detaillierte Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Spezifische Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	a. Bei Bedarf lassen sich die gültigen Felder für den `-fields` Parameter mit folgendem Befehl anzeigen: `volume show -fields ?` b. Die gewünschten Informationen werden mit dem `-fields` Parameter angezeigt: volume show -vserver vserver_name -fields fieldname,…

Beispiele

Das folgende Beispiel zeigt eine Zusammenfassung der eingebundenen und nicht eingebundenen Volumes auf SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

Das folgende Beispiel zeigt Informationen zu bestimmten Feldern für Volumes auf SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
```

```
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /              -
node3
```

Namenszuordnungen konfigurieren

Informationen zur Konfiguration der ONTAP SMB-Namenszuordnungen

ONTAP verwendet Namenszuordnung, um CIFS-Identitäten UNIX-Identitäten, Kerberos-Identitäten UNIX-Identitäten und UNIX-Identitäten CIFS-Identitäten zuzuordnen. Diese Informationen werden benötigt, um Benutzeranmeldeinformationen zu erhalten und den korrekten Dateizugriff bereitzustellen, unabhängig davon, ob die Verbindung von einem NFS-Client oder einem CIFS-Client erfolgt.

Es gibt zwei Ausnahmen, bei denen Sie keine Namenszuordnung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen nicht, CIFS-Zugriff oder den NTFS-Sicherheitsstil auf Volumes zu verwenden.
- Stattdessen wird der Standardbenutzer konfiguriert.

  In diesem Szenario ist keine Namenszuordnung erforderlich, da statt der Zuordnung jeder einzelnen Client-Anmeldeinformation alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass die Namenszuordnung nur für Benutzer und nicht für Gruppen verwendet werden kann.

Sie können jedoch eine Gruppe einzelner Benutzer einem bestimmten Benutzer zuordnen. Beispielsweise können alle AD-Benutzer, deren Name mit dem Wort SALES beginnt oder endet, einem bestimmten UNIX-Benutzer und der Benutzer-UID dieses Benutzers zugeordnet werden.

Informationen zur ONTAP SMB Namenszuordnung

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, prüft es zunächst die lokale Name-Mapping-Datenbank und den LDAP-Server auf eine vorhandene Zuordnung. Ob einer oder beide geprüft werden und in welcher Reihenfolge, wird durch die Namensdienstkonfiguration der SVM bestimmt.

- Zuordnung von Windows zu UNIX

  Wird keine Zuordnung gefunden, prüft ONTAP, ob der in Kleinbuchstaben geschriebene Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Falls dies nicht funktioniert, wird der standardmäßige UNIX-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-UNIX-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

- Für die UNIX-zu-Windows-Zuordnung

  Wird keine Zuordnung gefunden, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der Standard-SMB-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-CIFS-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

Maschinenkonten werden standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung der Maschinenkonten fehl.

- Ab ONTAP 9.5 ist es möglich, Maschinenkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuzuordnen.
- In ONTAP 9.4 und früher ist es nicht möglich, Maschinenkonten anderen Benutzern zuzuordnen.

  Selbst wenn Namenszuordnungen für Maschinenkonten definiert sind, werden die Zuordnungen ignoriert.

Informationen zu ONTAP SMB Multidomain-Suchen für die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen

ONTAP unterstützt die Suche in mehreren Domänen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle ermittelten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersetzungsmuster durchsucht, bis ein passendes Ergebnis gefunden wird. Alternativ ist es möglich, eine Liste bevorzugter vertrauenswürdiger Domänen zu konfigurieren, die anstelle der ermittelten vertrauenswürdigen Domänenliste verwendet und der Reihe nach durchsucht wird, bis ein passendes Ergebnis gefunden wird.

Wie Domänenvertrauensstellungen die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen beeinflussen

Um die Funktionsweise der domänenübergreifenden Benutzernamenszuordnung zu verstehen, ist es erforderlich, die Funktionsweise von Domänenvertrauensstellungen in Verbindung mit ONTAP zu verstehen. Active Directory-Vertrauensstellungen mit der Home-Domäne des CIFS-Servers können entweder eine bidirektionale Vertrauensstellung oder eine von zwei Arten unidirektionaler Vertrauensstellungen sein, entweder eine eingehende oder eine ausgehende Vertrauensstellung. Die Home-Domäne ist die Domäne, zu der der CIFS-Server auf der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Vertrauensstellungen vertrauen sich beide Domänen. Wenn die Heimatdomäne des CIFS-Servers eine bidirektionale Vertrauensstellung mit einer anderen Domäne hat, kann die Heimatdomäne einen Benutzer der vertrauenswürdigen Domäne authentifizieren und autorisieren und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen kann nur in Domänen mit bidirektionalen Vertrauensstellungen zwischen der Heimatdomäne und der anderen Domäne

durchgeführt werden.

- *Ausgehendes Vertrauen*

  Bei einer ausgehenden Vertrauensstellung vertraut die Heimatdomäne der anderen Domäne. In diesem Fall kann die Heimatdomäne einen Benutzer der ausgehend vertrauenswürdigen Domäne authentifizieren und autorisieren.

  Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer ausgehenden Vertrauensstellung zur Home-Domäne *nicht* durchsucht.

- *Eingehendes Vertrauen*

  Bei einer eingehenden Vertrauensstellung vertraut die andere Domäne der Heimatdomäne des CIFS-Servers. In diesem Fall kann die Heimatdomäne einen Benutzer der eingehenden vertrauenswürdigen Domäne weder authentifizieren noch autorisieren.

  Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer eingehenden Vertrauensstellung zur Heimatdomäne *nicht* durchsucht.

Wie Platzhalter (*) zur Konfiguration von multidomain Suchen für die Namenszuordnung verwendet werden

Die Suche nach domänenübergreifenden Namenszuordnungen wird durch die Verwendung von Platzhaltern im Domänenteil des Windows-Benutzernamens erleichtert. Die folgende Tabelle veranschaulicht, wie Platzhalter im Domänenteil eines Namenszuordnungseintrags verwendet werden können, um domänenübergreifende Suchen zu ermöglichen:

Muster	Ersatz	Ergebnis
root	*\\Administrator	Der UNIX-Benutzer “root” ist dem Benutzer “administrator” zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit dem Namen “administrator” gefunden wird.
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit diesem Namen gefunden wird.  Das Muster ** ist nur für die Namenszuordnung von UNIX nach Windows gültig, nicht umgekehrt.

Wie Suchvorgänge nach Namen mit mehreren Domänen durchgeführt werden

Es stehen zwei Methoden zur Verfügung, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für multidomain Name Searches verwendet wird:

- Die von ONTAP automatisch erstellte Liste der bidirektionalen Vertrauensstellungen kann verwendet werden
- Die bevorzugte Liste vertrauenswürdiger Domänen verwenden, die Sie zusammengestellt haben

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet wird, wobei für den Domänenteil des Benutzernamens ein Platzhalter verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt gesucht:

- Wenn eine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der angegebenen Reihenfolge gesucht.
- Wenn keine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Heimatdomäne gesucht.
- Wenn für die Heimatdomäne keine bidirektional vertrauenswürdigen Domänen vorhanden sind, wird der Benutzer in der Heimatdomäne gesucht.

Ab ONTAP 9.13.1 führt ONTAP bei der Suche nach vertrauenswürdigen Domänen während Namenszuordnungsvorgängen für mehrere Domänen eine Standortermittlung für diese vertrauenswürdigen Domänen durch und verwendet den ermittelten Standort für Domänencontroller-Abfragen. Dadurch wird sichergestellt, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für vertrauenswürdige Domänen fehlschlägt, verwendet ONTAP den Standardstandort des SMB-Servers.

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet ist, dessen Benutzername keinen Domänenteil enthält, wird der Windows-Benutzer in der Heimatdomäne gesucht.

Informationen zu den Konvertierungsregeln für die ONTAP SMB-Namenszuordnung

Ein ONTAP-System verwaltet für jede SVM einen Satz von Konvertierungsregeln. Jede Regel besteht aus zwei Teilen: einem Muster und einer Ersetzung. Die Konvertierung beginnt am Anfang der entsprechenden Liste und führt eine Ersetzung basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein regulärer Ausdruck im UNIX-Stil. Die Ersetzung ist eine Zeichenkette mit Escape-Sequenzen, die Teilausdrücke des Musters darstellen, analog zum UNIX `sed` Programm.

ONTAP SMB-Namenszuordnung erstellen

Sie können den `vserver name-mapping create` Befehl verwenden, um eine Namenszuordnung zu erstellen. Namenszuordnungen werden verwendet, damit Windows-Benutzer auf UNIX Security Style Volumes zugreifen können und umgekehrt.

Über diese Aufgabe

ONTAP unterstützt für jede SVM bis zu 12.500 Namenszuordnungen pro Richtung.

Schritt

1. Namenszuordnung erstellen: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text`

`-replacement` *text*

> Die `-pattern` und `-replacement`-Anweisungen können als reguläre Ausdrücke formuliert werden. Die `-replacement`-Anweisung kann auch verwendet werden, um dem Benutzer eine Zuordnung explizit zu verweigern, indem die Null-Ersetzungszeichenkette `" "` (das Leerzeichen) verwendet wird. Weitere Informationen zu `vserver name-mapping create` finden sich in der "ONTAP-Befehlsreferenz".

Wenn Windows-zu-UNIX-Zuordnungen erstellt werden, müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, ausloggen und sich erneut anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Der folgende Befehl erstellt eine Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätsliste. Die Zuordnung ordnet den UNIX-Benutzer johnd dem Windows-Benutzer ENG\JohnDoe zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätsliste. Hier beinhalten Muster und Ersetzung reguläre Ausdrücke. Die Zuordnung ordnet jeden CIFS-Benutzer in der Domäne ENG Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Das Muster enthält hierbei das Zeichen “$” im Windows-Benutzernamen, das maskiert werden muss. Die Zuordnung ordnet den Windows-Benutzer ENG\john$ops dem UNIX-Benutzer john_ops zu.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Den standardmäßigen ONTAP SMB-Benutzer konfigurieren

Sie können einen Standardbenutzer konfigurieren, der verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie keine einzelnen Benutzer zwischen UNIX und Windows zuordnen möchten. Alternativ sollte kein Standardbenutzer konfiguriert werden, wenn die Authentifizierung nicht zugeordneter Benutzer fehlschlagen soll.

Über diese Aufgabe

Für die CIFS Authentifizierung kann anstelle der Zuordnung jedes Windows-Benutzers zu einem einzelnen UNIX-Benutzer ein Standard-UNIX-Benutzer angegeben werden.

Für die NFS Authentifizierung kann anstelle der Zuordnung jedes UNIX-Benutzers zu einem einzelnen Windows-Benutzer ein Standard-Windows-Benutzer angegeben werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Den Standard-UNIX-Benutzer konfigurieren	`vserver cifs options modify -default -unix-user user_name`
Den Standard-Windows-Benutzer konfigurieren	`vserver nfs modify -default-win-user user_name`

ONTAP Befehle zur Verwaltung von SMB-Namenszuordnungen

Für die Verwaltung von Namenszuordnungen gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Namenszuordnung erstellen	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Anzeigenamenzuordnungen anzeigen	`vserver name-mapping show`
Die Position zweier Namenszuordnungen wird getauscht. HINWEIS: Ein Tausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Eine Namenszuordnung ändern	`vserver name-mapping modify`
Eine Namenszuordnung löschen	`vserver name-mapping delete`
Die korrekte Namenszuordnung validieren	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

Konfiguration von Namenszuordnungssuchen über mehrere Domänen hinweg

Aktivieren oder Deaktivieren von ONTAP SMB Multidomain-Namenszuordnungssuchen

Bei der Suche nach domänenübergreifenden Namenszuordnungen kann im Domänenteil eines Windows-Namens beim Konfigurieren der Zuordnung von UNIX-Benutzernamen zu

Windows-Benutzernamen ein Platzhalterzeichen (**) verwendet werden. Durch die Verwendung eines Platzhalterzeichens (*) im Domänenteil des Namens kann ONTAP alle Domänen durchsuchen, die eine bidirektionale Vertrauensstellung mit der Domäne haben, die das Computerkonto des CIFS-Servers enthält.

Über diese Aufgabe

Als Alternative zur Suche in allen bidirektional vertrauenswürdigen Domänen kann eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert werden. Wenn eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert ist, verwendet ONTAP diese Liste anstelle der ermittelten bidirektional vertrauenswürdigen Domänen, um multidomain Namenszuordnungs-Suchen durchzuführen.

- Die Suche nach domänenübergreifenden Namenszuordnungen ist standardmäßig aktiviert.
- Diese Option ist auf der Stufe „Erweitertes Berechtigungsniveau“ verfügbar.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die Suche nach Multidomain-Namenszuordnungen durchgeführt wird…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

Verfügbare Serveroptionen

Vertrauenswürdige ONTAP SMB-Domänen zurücksetzen und neu erkennen

Sie können die erneute Erkennung aller vertrauenswürdigen Domänen erzwingen. Dies kann nützlich sein, wenn die Server der vertrauenswürdigen Domänen nicht angemessen reagieren oder sich die Vertrauensstellungen geändert haben. Es werden nur Domänen erkannt, die über eine bidirektionale Vertrauensstellung zur Heimatdomäne verfügen, also der Domäne, die das Computerkonto des CIFS-Servers enthält.

Ab ONTAP 9.13.1 führt ONTAP bei der erneuten Erkennung vertrauenswürdiger Domänen auch eine Standortermittlung für diese vertrauenswürdigen Domänen durch. ONTAP verwendet die ermittelten Standortinformationen für Domänencontroller-Abfragen vertrauenswürdiger Domänen. Dies trägt dazu bei, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für eine vertrauenswürdige Domäne fehlschlägt, verwendet ONTAP den Standardstandort des SMB-Servers.

Schritt

1. Vertrauenswürdige Domänen werden mithilfe des `vserver cifs domain trusts rediscover` Befehls zurückgesetzt und neu erkannt.

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

Verwandte Informationen

Informationen zu erkannten vertrauenswürdigen Domänen anzeigen

Informationen zu erkannten vertrauenswürdigen ONTAP SMB-Domänen

Sie können Informationen zu den ermittelten vertrauenswürdigen Domänen für die Heimatdomäne des CIFS-Servers anzeigen, also die Domäne, die das Computerkonto des CIFS-Servers enthält. Dies kann hilfreich sein, wenn Sie wissen möchten, welche vertrauenswürdigen Domänen ermittelt wurden und wie sie in der Liste der ermittelten vertrauenswürdigen Domänen angeordnet sind.

Über diese Aufgabe

Es werden nur Domänen mit bidirektionalen Vertrauensstellungen zur Heimatdomäne ermittelt. Da der Domänencontroller (DC) der Heimatdomäne die Liste der vertrauenswürdigen Domänen in einer vom DC festgelegten Reihenfolge zurückgibt, lässt sich die Reihenfolge der Domänen in der Liste nicht vorhersagen. Durch die Anzeige der Liste der vertrauenswürdigen Domänen lässt sich die Suchreihenfolge für Namenszuordnungen in mehreren Domänen ermitteln.

Ab ONTAP 9.13.1 führt ONTAP auch eine Standortermittlung für vertrauenswürdige Domänen durch und verwendet den ermittelten Standort, um Domänencontroller für diese Domänen zu finden. Dies trägt dazu bei, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für eine vertrauenswürdige Domäne fehlschlägt, greift ONTAP auf den Standardstandort des SMB-Servers zurück.

Die angezeigten Informationen zur vertrauenswürdigen Domäne sind nach Knoten und Storage Virtual Machine (SVM) gruppiert.

Schritt

1. Informationen über erkannte vertrauenswürdige Domänen werden mit dem `vserver cifs domain trusts show` Befehl angezeigt.

   ```
   vserver cifs domain trusts show -vserver vs1
   ```

   ```
      Node: node1
   Vserver: vs1

   Home Domain             Trusted Domain
   ---------------------   ----------------------------------
   EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                           CIFS2.EXAMPLE.COM
                           EXAMPLE.COM

      Node: node2
   Vserver: vs1
   ```

```
Home Domain             Trusted Domain
--------------------  ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

Verwandte Informationen

Vertrauenswürdige Domänen zurücksetzen und neu erkennen

Vertrauenswürdige ONTAP SMB-Domänen in bevorzugten Listen hinzufügen, entfernen oder ersetzen

Sie können vertrauenswürdige Domänen zur Liste der bevorzugten vertrauenswürdigen Domänen für den SMB-Server hinzufügen oder daraus entfernen oder die aktuelle Liste bearbeiten. Wenn eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert ist, wird diese Liste anstelle der ermittelten bidirektionalen vertrauenswürdigen Domänen bei multidomänenübergreifenden Namenszuordnungs-Suchen verwendet.

Über diese Aufgabe

- Wenn Sie einer bestehenden Liste vertrauenswürdige Domänen hinzufügen, wird die neue Liste mit der bestehenden Liste zusammengeführt, wobei die neuen Einträge am Ende eingefügt werden. Die vertrauenswürdigen Domänen werden in der Reihenfolge durchsucht, in der sie in der Liste der vertrauenswürdigen Domänen erscheinen.
- Wenn Sie vertrauenswürdige Domänen aus der bestehenden Liste entfernen und keine Liste angeben, wird die gesamte Liste der vertrauenswürdigen Domänen für die angegebene Storage Virtual Machine (SVM) entfernt.
- Wenn die bestehende Liste der vertrauenswürdigen Domänen geändert wird, überschreibt die neue Liste die bestehende Liste.

> Sie sollten in der Liste der bevorzugten vertrauenswürdigen Domänen nur bidirektional vertrauenswürdige Domänen eintragen. Obwohl Sie ausgehende oder eingehende Vertrauensstellungen in die bevorzugte Domänenliste eintragen können, werden diese bei der Durchführung von multidomain Namenszuordnungs-Suchen nicht verwendet. ONTAP überspringt den Eintrag für die unidirektionale Domäne und fährt mit der nächsten bidirektional vertrauenswürdigen Domäne in der Liste fort.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domänen durchführen möchten…	Verwenden Sie den Befehl…
Vertrauenswürdige Domänen zur Liste hinzufügen	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Vertrauenswürdige Domänen aus der Liste entfernen	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domänen durchführen möchten…	Verwenden Sie den Befehl…
Die bestehende Liste bearbeiten	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Beispiele

Der folgende Befehl fügt zwei vertrauenswürdige Domänen (cifs1.example.com und cifs2.example.com) zur Liste der bevorzugten vertrauenswürdigen Domänen hinzu, die von SVM vs1 verwendet wird:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Der folgende Befehl entfernt zwei vertrauenswürdige Domänen aus der von SVM vs1 verwendeten Liste:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Der folgende Befehl ändert die von SVM vs1 verwendete Liste vertrauenswürdiger Domänen. Die neue Liste ersetzt die ursprüngliche Liste:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Verwandte Informationen

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen

Informationen zur bevorzugten vertrauenswürdigen ONTAP SMB-Domänenliste anzeigen

Sie können Informationen darüber anzeigen, welche vertrauenswürdigen Domänen in der Liste der bevorzugten vertrauenswürdigen Domänen enthalten sind und in welcher Reihenfolge sie durchsucht werden, wenn multidomain Namenszuordnungs-Suchen aktiviert sind. Eine bevorzugte vertrauenswürdige Domänenliste kann als Alternative zur automatisch ermittelten Liste vertrauenswürdiger Domänen konfiguriert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen zu Folgendem angezeigt werden sollen…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen im Cluster, gruppiert nach Storage Virtual Machine (SVM)	`vserver cifs domain name-mapping-search show`

Wenn Informationen zu Folgendem angezeigt werden sollen…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen für eine bestimmte SVM	`vserver cifs domain name-mapping-search show -vserver vserver_name`

Der folgende Befehl zeigt Informationen zu allen bevorzugten vertrauenswürdigen Domänen im Cluster an:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Verwandte Informationen

Vertrauenswürdige Domänen in bevorzugten Listen hinzufügen, entfernen oder ersetzen

SMB-Freigaben erstellen und konfigurieren

Informationen zum Erstellen und Konfigurieren von ONTAP SMB-Freigaben

Bevor Benutzer und Anwendungen über SMB auf Daten auf dem CIFS-Server zugreifen können, müssen SMB-Shares erstellt und konfiguriert werden, was einen benannten Zugriffspunkt in einem Volume darstellt. Shares können angepasst werden, indem Share-Parameter und Share-Eigenschaften angegeben werden. Eine vorhandene Share kann jederzeit geändert werden.

Wenn eine SMB-Freigabe erstellt wird, erstellt ONTAP standardmäßig eine ACL für die Freigabe mit Vollzugriffsberechtigungen für Everyone.

SMB-Freigaben sind an den CIFS-Server auf der Storage Virtual Machine (SVM) gebunden. SMB-Freigaben werden gelöscht, wenn entweder die SVM gelöscht wird oder der mit ihr verbundene CIFS-Server von der SVM gelöscht wird. Wird der CIFS-Server auf der SVM neu erstellt, müssen die SMB-Freigaben ebenfalls neu erstellt werden.

Verwandte Informationen

- Informationen zu lokalen Benutzern und Gruppen
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren

Informationen zu den standardmäßigen administrativen ONTAP SMB-Freigaben

Wenn Sie einen CIFS-Server auf Ihrer Storage Virtual Machine (SVM) erstellen, werden automatisch standardmäßige administrative Freigaben angelegt. Es ist wichtig zu verstehen, was diese Standardfreigaben sind und wie sie verwendet werden.

ONTAP erstellt beim Erstellen des CIFS-Servers die folgenden standardmäßigen administrativen Freigaben:

Ab ONTAP 9.8 wird die admin$ Freigabe nicht mehr standardmäßig erstellt.

- ipc$
- admin$ (nur ONTAP 9.7 und älter)
- c$

Da Freigaben, die mit dem $-Zeichen enden, versteckte Freigaben sind, sind die standardmäßigen administrativen Freigaben nicht über „Arbeitsplatz“ sichtbar, sie lassen sich jedoch über „Freigegebene Ordner“ anzeigen.

Wie die Standardfreigaben ipc$ und admin$ verwendet werden

Die Freigaben ipc$ und admin$ werden von ONTAP verwendet und können von Windows-Administratoren nicht genutzt werden, um auf Daten zuzugreifen, die sich auf der SVM befinden.

- ipc$ Freigabe

  Die ipc$-Freigabe ist eine Ressource, die die für die Kommunikation zwischen Programmen unerlässlichen Named Pipes freigibt. Die ipc$-Freigabe wird während der Remote-Administration eines Computers und beim Anzeigen der freigegebenen Ressourcen eines Computers verwendet. Die Freigabeeinstellungen, Freigabeeigenschaften oder ACLs der ipc$-Freigabe können nicht geändert werden. Die ipc$-Freigabe kann auch nicht umbenannt oder gelöscht werden.

- admin$ Freigabe (nur ONTAP 9.7 und früher)

  Ab ONTAP 9.8 wird die admin$ Freigabe nicht mehr standardmäßig erstellt.

  Die administrative Freigabe admin$ wird während der Remote-Administration der SVM verwendet. Der Pfad dieser Ressource ist immer der Pfad zum SVM-Root. Die Freigabeeinstellungen, Freigabeeigenschaften oder ACLs für die administrative Freigabe admin$ können nicht geändert werden. Auch das Umbenennen oder Löschen der administrativen Freigabe admin$ ist nicht möglich.

Wie die Standardfreigabe c$ verwendet wird

Die c$ Freigabe ist eine administrative Freigabe, die der Cluster- oder SVM-Administrator verwenden kann, um auf das SVM Root-Volume zuzugreifen und es zu verwalten.

Die folgenden Merkmale kennzeichnen die c$ administrative Freigabe:

- Der Pfad für diese Freigabe ist immer der Pfad zum SVM-Root-Volume und kann nicht geändert werden.
- Die Standard-ACL für die c$ Freigabe ist Administrator / Vollzugriff.

  Dieser Benutzer ist der BUILTIN\administrator. Standardmäßig kann der BUILTIN\administrator auf die Freigabe zugreifen und Dateien und Ordner im zugeordneten Stammverzeichnis anzeigen, erstellen, ändern oder löschen. Beim Verwalten von Dateien und Ordnern in diesem Verzeichnis ist Vorsicht geboten.

- Sie können die ACL der c$ Freigabe ändern.
- Sie können die Einstellungen und Eigenschaften der C$-Freigabe ändern.
- Sie können die c$ Freigabe nicht löschen.
- Der SVM-Administrator kann vom zugeordneten c$ Share aus über die Namensraumübergänge auf den Rest des SVM-Namensraums zugreifen.
- Auf die c$ Freigabe kann über die Microsoft Management Console zugegriffen werden.

Verwandte Informationen

Erweiterte Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit konfigurieren

Informationen zu den Anforderungen an die Benennung von ONTAP SMB-Freigaben

Die ONTAP Anforderungen an die Benennung von Freigaben sind bei der Erstellung von SMB-Freigaben auf dem SMB-Server zu berücksichtigen.

Die Namenskonventionen für Freigaben unter ONTAP sind die gleichen wie unter Windows und umfassen die folgenden Anforderungen:

- Der Name jeder Freigabe muss für den SMB-Server eindeutig sein.
- Bei Share-Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- Die maximale Länge des Freigabenamens beträgt 80 Zeichen.
- Unicode-Freigabenamen werden unterstützt.
- Freigabenamen, die mit dem $-Zeichen enden, sind versteckte Freigaben.
- Bei ONTAP 9.7 und früheren Versionen werden die administrativen Freigaben admin$, ipc$ und c$ automatisch auf jedem CIFS-Server erstellt und sind reservierte Freigabenamen. Ab ONTAP 9.8 wird die Freigabe admin$ nicht mehr automatisch erstellt.
- Der Freigabename ONTAP_ADMIN$ kann beim Erstellen einer Freigabe nicht verwendet werden.
- Freigabenamen, die Leerzeichen enthalten, werden unterstützt:
  - Ein Leerzeichen darf weder als erstes noch als letztes Zeichen in einem Freigabenamen verwendet werden.
  - Freigabenamen, die ein Leerzeichen enthalten, müssen in Anführungszeichen gesetzt werden.

    Einfache Anführungszeichen gelten als Bestandteil des Freigabenamens und können nicht anstelle von Anführungszeichen verwendet werden.

- Folgende Sonderzeichen werden bei der Benennung von SMB-Freigaben unterstützt:

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- Die folgenden Sonderzeichen sind bei der Benennung von SMB-Freigaben nicht zulässig:

```
** [ ] " / \ : ; | < > , ? * =
```

Informationen zu den Anforderungen an die Groß-/Kleinschreibung von ONTAP SMB-Verzeichnissen beim Erstellen von Freigaben in einer Multiprotokollumgebung

Wenn Sie Freigaben in einer SVM erstellen, in der das 8.3-Namensschema verwendet wird, um zwischen Verzeichnisnamen zu unterscheiden, bei denen es nur Unterschiede in der Groß-/Kleinschreibung gibt, muss der 8.3-Name im Freigabepfad verwendet werden, damit der Client mit dem gewünschten Verzeichnispfad verbunden wird.

Im folgenden Beispiel wurden auf einem Linux-Client zwei Verzeichnisse mit den Namen „testdir“ und „TESTDIR“ erstellt. Der Verbindungspfad des Volumes, das die Verzeichnisse enthält, ist `/home`. Die erste

Ausgabe stammt von einem Linux-Client, die zweite Ausgabe von einem SMB-Client.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Wenn Sie eine Freigabe für das zweite Verzeichnis erstellen, muss im Freigabepfad der 8.3-Name verwendet werden. In diesem Beispiel ist der Freigabepfad zum ersten Verzeichnis `/home/testdir` und der Freigabepfad zum zweiten Verzeichnis ist `/home/TESTDI~1`.

Freigabeeigenschaften zu bestehenden ONTAP SMB-Freigaben hinzufügen oder entfernen

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften hinzufügen oder entfernen.

Die verfügbaren Freigabeeigenschaften sind wie folgt:

Freigabeeigenschaften	Beschreibung
`oplocks`	Diese Eigenschaft legt fest, dass die Freigabe opportunistische Sperren verwendet, auch bekannt als Client-seitiges Caching.
`browsable`	Diese Eigenschaft ermöglicht Windows-Clients das Durchsuchen der Freigabe.
`showsnapshot`	Diese Eigenschaft legt fest, dass Snapshots von Clients angezeigt und durchsucht werden können.
`changenotify`	Diese Eigenschaft gibt an, dass die Freigabe Change Notify-Anforderungen unterstützt. Für Freigaben auf einer SVM ist dies eine standardmäßige Anfangseigenschaft.
`attributecache`	Diese Eigenschaft aktiviert das Caching von Dateiattributen auf der SMB-Freigabe, um einen schnelleren Zugriff auf Attribute zu ermöglichen. Standardmäßig ist das Attribut-Caching deaktiviert. Diese Eigenschaft sollte nur aktiviert werden, wenn Clients über SMB 1.0 auf Freigaben zugreifen. Diese Freigabeeigenschaft ist nicht anwendbar, wenn Clients über SMB 2.x oder SMB 3.0 auf Freigaben zugreifen.
`continuously-available`	Diese Eigenschaft ermöglicht es SMB-Clients, die sie unterstützen, Dateien dauerhaft zu öffnen. Dateien, die auf diese Weise geöffnet werden, sind vor Störungen wie Failover und Giveback geschützt.

Freigabeeigenschaften	Beschreibung
`branchcache`	Diese Eigenschaft legt fest, dass die Freigabe es Clients ermöglicht, BranchCache-Hashwerte für die Dateien innerhalb dieser Freigabe anzufordern. Diese Option ist nur relevant, wenn „per-share“ als Betriebsmodus in der CIFS BranchCache-Konfiguration angegeben wird.
`access-based-enumeration`	Diese Eigenschaft legt fest, dass *Access Based Enumeration* (ABE) für diese Freigabe aktiviert ist. ABE-gefilterte freigegebene Ordner sind für einen Benutzer basierend auf dessen individuellen Zugriffsrechten sichtbar, wodurch die Anzeige von Ordnern oder anderen freigegebenen Ressourcen verhindert wird, auf die der Benutzer keine Zugriffsrechte hat.
`namespace-caching`	Diese Eigenschaft legt fest, dass SMB-Clients, die sich mit dieser Freigabe verbinden, die von den CIFS-Servern zurückgegebenen Ergebnisse der Verzeichnisauflistung zwischenspeichern können, was die Leistung verbessern kann. Standardmäßig speichern SMB 1 Clients keine Ergebnisse der Verzeichnisauflistung. Da SMB 2 und SMB 3 Clients die Ergebnisse der Verzeichnisauflistung standardmäßig zwischenspeichern, bietet die Angabe dieser Freigabeeigenschaft nur SMB 1 Clientverbindungen Leistungsvorteile.
`encrypt-data`	Diese Eigenschaft legt fest, dass beim Zugriff auf diese Freigabe SMB-Verschlüsselung verwendet werden muss. SMB-Clients, die keine Verschlüsselung beim Zugriff auf SMB-Daten unterstützen, haben keinen Zugriff auf diese Freigabe.

Fügen Sie Freigabeeigenschaften zu bestehenden ONTAP SMB-Shares hinzu

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften hinzufügen. Dies kann hilfreich sein, wenn Sie die Freigabekonfiguration an geänderte Anforderungen in Ihrer Umgebung anpassen möchten.

Bevor Sie beginnen

Die Freigabe, deren Eigenschaften Sie ändern möchten, muss vorhanden sein.

Über diese Aufgabe

- Es besteht die Möglichkeit, eine oder mehrere Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste hinzuzufügen.
- Alle zuvor festgelegten Share-Eigenschaften bleiben bestehen.

  Neu hinzugefügte Eigenschaften werden der bestehenden Liste der Share-Eigenschaften hinzugefügt.
- Wenn für bereits auf die Freigabe angewendete Freigabeeigenschaften ein neuer Wert angegeben wird, ersetzt der neu angegebene Wert den ursprünglichen Wert.
- Sie können Freigabeeigenschaften mit dem `vserver cifs share properties add`Befehl nicht entfernen.

  Mit dem `vserver cifs share properties remove` Befehl lassen sich Freigabeeigenschaften entfernen.

Schritte

1. Freigabeeigenschaften hinzufügen:

```
vserver cifs share properties add -vserver <SVM_name> -share-name
<share_name> -share-properties <properties>,...
```

2. Überprüfen Sie die Einstellungen der Freigabeeigenschaften:

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

Beispiel

Der folgende Befehl fügt die `showsnapshot`Share-Eigenschaft zu einer Freigabe mit dem Namen “share1” auf SVM vs1 hinzu:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

Entfernen Sie die Freigabeeigenschaften bestehender ONTAP SMB-Freigaben

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften entfernen. Dies kann hilfreich sein, wenn Sie die Freigabekonfiguration an geänderte Anforderungen in Ihrer Umgebung anpassen möchten.

Über diese Aufgabe

- Sie können eine oder mehrere Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste entfernen.
- Alle zuvor festgelegten, aber nicht entfernten Freigabeeigenschaften bleiben weiterhin wirksam.

Schritte

1. Eigenschaften der Freigabe entfernen:

```
vserver cifs share properties remove -vserver <SVM_name> -share-name
<share_name> -share-properties <properties>,...
```

2. Überprüfen Sie die Einstellungen der Freigabeeigenschaften:

```
vserver cifs share show -vserver <SVM_name> -share-name <share_name>
```

Beispiel

Der folgende Befehl entfernt die `browsable` Freigabeeigenschaft von einer Freigabe mit dem Namen “share2” auf SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Verwandte Informationen

Befehle zur Verwaltung von Freigaben

ONTAP SMB-Benutzerzugriff mit der Einstellung „force-group share“ optimieren

Wenn Sie über die ONTAP Befehlszeile eine Freigabe für Daten mit effektiver UNIX-Sicherheit erstellen, kann festgelegt werden, dass alle von SMB-Benutzern in dieser Freigabe erstellten Dateien derselben Gruppe angehören, der sogenannten *force-group*, die eine vordefinierte Gruppe in der UNIX-Gruppendatenbank sein muss. Die Verwendung einer Force-Group vereinfacht es, sicherzustellen, dass Dateien von SMB-Benutzern aus verschiedenen Gruppen abgerufen werden können.

Die Angabe einer Force-Gruppe ist nur dann sinnvoll, wenn sich die Freigabe in einem UNIX- oder gemischten qtree befindet. Für Freigaben in einem NTFS-Volume oder qtree ist keine Force-Gruppe erforderlich, da der Zugriff auf Dateien in diesen Freigaben durch Windows-Berechtigungen und nicht durch UNIX-GIDs bestimmt wird.

Wenn für eine Freigabe eine Force-Gruppe festgelegt wurde, gilt für diese Freigabe Folgendes:

- SMB-Benutzer in der Force-Gruppe, die auf diese Freigabe zugreifen, werden vorübergehend auf die GID der Force-Gruppe geändert.

  Diese GID ermöglicht ihnen den Zugriff auf Dateien in dieser Freigabe, die mit ihrer primären GID oder UID normalerweise nicht zugänglich sind.

- Alle von SMB-Benutzern in dieser Freigabe erstellten Dateien gehören derselben Force-Gruppe an, unabhängig von der primären GID des Dateibesitzers.

Wenn SMB-Benutzer versuchen, auf eine von NFS erstellte Datei zuzugreifen, bestimmen die primären GIDs der SMB-Benutzer die Zugriffsrechte.

Die Force-Gruppe hat keinen Einfluss darauf, wie NFS-Benutzer auf Dateien in dieser Freigabe zugreifen. Eine

von NFS erstellte Datei erhält die GID vom Dateibesitzer. Die Zugriffsberechtigungen werden anhand der UID und der primären GID des NFS-Benutzers bestimmt, der versucht, auf die Datei zuzugreifen.

Die Verwendung einer Force-Group vereinfacht es, sicherzustellen, dass Dateien von SMB-Benutzern aus verschiedenen Gruppen abgerufen werden können. Wenn beispielsweise eine Freigabe erstellt werden soll, um die Webseiten des Unternehmens zu speichern und Benutzern aus den Abteilungen Engineering und Marketing Schreibzugriff zu gewähren, kann eine Freigabe erstellt und der Force-Group mit dem Namen „webgroup1“ Schreibzugriff erteilt werden. Aufgrund der Force-Group gehören alle von SMB-Benutzern in dieser Freigabe erstellten Dateien der Gruppe „webgroup1“. Zusätzlich wird Benutzern beim Zugriff auf die Freigabe automatisch die GID der Gruppe „webgroup1“ zugewiesen. So können alle Benutzer auf diese Freigabe schreiben, ohne dass die Zugriffsrechte der Benutzer in den Abteilungen Engineering und Marketing verwaltet werden müssen.

Verwandte Informationen

Freigaben mit der Einstellung „force-group share“ erstellen

ONTAP SMB-Freigaben mit der Einstellung „force-group share“ erstellen

Eine SMB-Freigabe mit der Einstellung „force-group share“ kann erstellt werden, wenn SMB-Benutzer, die auf Daten auf Volumes oder Qtrees mit UNIX-Dateisicherheit zugreifen, von ONTAP als Mitglieder derselben UNIX-Gruppe betrachtet werden sollen.

Schritt

1. Die SMB-Freigabe wird erstellt: `vserver cifs share create -vserver vserver_name -share -name share_name -path path -force-group-for-create UNIX_group_name`

   Wenn der UNC-Pfad (`\\servername\sharename\filepath`) der Freigabe mehr als 256 Zeichen enthält (ohne das anfängliche „`\\`“ im UNC-Pfad), ist die Registerkarte **Sicherheit** im Windows-Eigenschaftenfenster nicht verfügbar. Dies ist ein Problem des Windows-Clients und nicht von ONTAP. Um dieses Problem zu vermeiden, sollten keine Freigaben mit UNC-Pfaden erstellt werden, die mehr als 256 Zeichen enthalten.

   Wenn die Erzwingungsgruppe nach der Erstellung der Freigabe entfernt werden soll, kann die Freigabe jederzeit bearbeitet und eine leere Zeichenfolge ("") als Wert für den `-force-group-for-create` Parameter angegeben werden. Wenn die Erzwingungsgruppe durch Bearbeiten der Freigabe entfernt wird, behalten alle bestehenden Verbindungen zu dieser Freigabe die zuvor festgelegte Erzwingungsgruppe als primäre GID bei.

Beispiel

Der folgende Befehl erstellt eine Freigabe „`webpages`“, die im Web im `/corp/companyinfo` Verzeichnis zugänglich ist, in dem alle Dateien, die SMB-Benutzer erstellen, der Gruppe webgroup1 zugewiesen werden:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Verwandte Informationen

Benutzerzugriff mit der Einstellung „force-group share“ optimieren

Informationen zu ONTAP SMB-Freigaben mit der MMC anzeigen

Informationen zu SMB-Freigaben auf Ihrer SVM lassen sich anzeigen und einige Verwaltungsaufgaben mithilfe der Microsoft Management Console (MMC) durchführen.

Zum Anzeigen der Freigaben ist eine Verbindung der MMC mit der SVM erforderlich.

Über diese Aufgabe

Mit der MMC lassen sich die folgenden Aufgaben für in SVMs enthaltene Freigaben durchführen:

- Freigaben anzeigen
- Aktive Sitzungen anzeigen
- Offene Dateien anzeigen
- Die Liste der Sitzungen, Dateien und Baumverbindungen im System wird aufgezählt.
- Offene Dateien im System schließen
- Offene Sitzungen schließen
- Freigaben erstellen/verwalten

> Die von den vorherigen Funktionen angezeigten Ansichten sind knotenspezifisch und nicht clusterspezifisch. Daher wird bei Verwendung der MMC zur Verbindung mit dem SMB-Server-Hostnamen (das heißt cifs01.domain.local) abhängig von der DNS-Konfiguration zu einer einzelnen LIF innerhalb des Clusters weitergeleitet.

Die folgenden Funktionen werden in MMC für ONTAP nicht unterstützt:

- Erstellen neuer lokaler Benutzer/Gruppen
- Verwaltung/Anzeige bestehender lokaler Benutzer/Gruppen
- Anzeigen von Ereignissen oder Leistungsprotokollen
- Storage
- Dienste und Anwendungen

In Fällen, in denen die Operation nicht unterstützt wird, können Sie `remote procedure call failed`Fehler erleben.

"Häufig gestellte Fragen: Verwendung der Windows MMC mit ONTAP"

Schritte

1. Die Computer Management MMC auf einem beliebigen Windows Server wird in der **Systemsteuerung** unter **Verwaltung** > **Computerverwaltung** geöffnet.
2. **Aktion** > **Mit einem anderen Computer verbinden** auswählen.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.
3. Den Namen des Speichersystems eingeben oder auf **Durchsuchen** klicken, um das Speichersystem zu finden.
4. Klicken Sie auf **OK**.

   Der MMC stellt eine Verbindung zum SVM her.
5. Im Navigationsbereich auf **Freigegebene Ordner** > **Freigaben** klicken.

   Im rechten Anzeigebereich wird eine Liste der Shares auf der SVM angezeigt.

6. Die Freigabeeigenschaften einer Freigabe werden angezeigt, wenn auf die Freigabe doppelt geklickt wird, wodurch das Dialogfeld **Eigenschaften** geöffnet wird.
7. Wenn keine Verbindung zum Speichersystem über die MMC möglich ist, kann der Benutzer der Gruppe BUILTIN\Administrators oder BUILTIN\Power Users auf dem Speichersystem mit einem der folgenden Befehle hinzugefügt werden:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

ONTAP Befehle zur Verwaltung von SMB-Freigaben

Sie verwenden die `vserver cifs share`- und `vserver cifs share properties` -Befehle, um SMB-Freigaben zu verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen Sie eine SMB-Freigabe	`vserver cifs share create`
SMB-Freigaben anzeigen	`vserver cifs share show`
Ändern einer SMB-Freigabe	`vserver cifs share modify`
Eine SMB-Freigabe löschen	`vserver cifs share delete`
Freigabeeigenschaften zu einer bestehenden Freigabe hinzufügen	`vserver cifs share properties add`
Freigabeeigenschaften von einer bestehenden Freigabe entfernen	`vserver cifs share properties remove`
Informationen zu Aktieneigenschaften	`vserver cifs share properties show`

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

Sicherer Dateizugriff mithilfe von SMB-Freigabe-ACLs

Informationen zur Verwaltung von ONTAP SMB-ACLs auf Freigabeebene

Sie können die Zugriffssteuerungslisten (ACLs) auf Freigabeebene ändern, um Benutzern mehr oder weniger Zugriffsrechte auf die Freigabe zu gewähren. Sie können die ACLs auf Freigabeebene entweder mit Windows-Benutzern und -Gruppen oder mit UNIX-Benutzern und -Gruppen konfigurieren.

Standardmäßig gewährt die Freigabe-ACL der Standardgruppe „Jeder“ Vollzugriff. Vollzugriff in der ACL bedeutet, dass alle Benutzer in der Domäne und alle vertrauenswürdigen Domänen uneingeschränkten Zugriff auf die Freigabe haben. Das Zugriffslevel einer Freigabe-ACL lässt sich über die Microsoft Management Console (MMC) auf einem Windows-Client oder die ONTAP Befehlszeile steuern. "Freigabe-Zugriffskontrolllisten erstellen".

Bei der Verwendung des MMC gelten folgende Richtlinien:

- Die angegebenen Benutzer- und Gruppennamen müssen Windows-Namen sein.
- Es können nur Windows-Berechtigungen angegeben werden.

Die folgenden Richtlinien gelten bei Verwendung der ONTAP Befehlszeile:

- Die angegebenen Benutzer- und Gruppennamen können Windows-Namen oder UNIX-Namen sein.

  Wenn beim Erstellen oder Ändern von ACLs kein Benutzer- und Gruppentyp angegeben wird, ist der Standardtyp Windows-Benutzer und -Gruppen.

- Es können nur Windows-Berechtigungen angegeben werden.

Erstellen von ONTAP SMB-Freigabe-Zugriffssteuerungslisten

Die Konfiguration von Freigabeberechtigungen durch das Erstellen von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben ermöglicht die Kontrolle der Zugriffsebene auf eine Freigabe für Benutzer und Gruppen.

Über diese Aufgabe

Sie können Zugriffssteuerungslisten auf Freigabeebene konfigurieren, indem Sie lokale oder Domänen-Windows-Benutzer- oder Gruppennamen oder UNIX-Benutzer- oder Gruppennamen verwenden.

Bevor Sie eine neue ACL erstellen, sollten Sie die standardmäßige Freigabe-ACL `Everyone / Full Control` löschen, da diese ein Sicherheitsrisiko darstellt.

Im Arbeitsgruppenmodus ist der lokale Domänenname der SMB-Servername.

Schritte

1. Die Standard-Freigabe-ACL löschen: `vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group Everyone`
2. Die neue Zugriffssteuerungsliste (ACL) konfigurieren:

Wenn Sie Zugriffssteuerungslisten (ACLs) mithilfe von… konfigurieren möchten	Geben Sie den Befehl ein…
Windows Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windows Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`

Wenn Sie Zugriffssteuerungslisten (ACLs) mithilfe von… konfigurieren möchten	Geben Sie den Befehl ein…
UNIX-Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIX-Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Es kann überprüft werden, ob die auf die Freigabe angewendete Zugriffssteuerungsliste (ACL) korrekt ist, indem der `vserver cifs share access-control show` Befehl verwendet wird.

Beispiel

Der folgende Befehl erteilt `Change` der Windows-Gruppe “Sales Team” Berechtigungen für die Freigabe “sales” auf der “vs1.example.com”-SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

Der folgende Befehl erteilt `Read` der UNIX-Gruppe „engineering“ die Berechtigung für die Freigabe „eng“ auf der SVM „vs2.example.com“:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
```

```
Vserver          Name        Name                    Type
Permission
---------------- ----------- ------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

Die folgenden Befehle erteilen `Change`der lokalen Windows-Gruppe „Tiger Team“ und `Full_Control`dem lokalen Windows-Benutzer „Sue Chang“ die Berechtigung für die Freigabe „datavol5“ auf der SVM „vs1“:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

ONTAP Befehle zur Verwaltung von SMB-Freigabezugriffskontrolllisten

Sie müssen die Befehle zur Verwaltung von SMB-Zugriffskontrolllisten (ACLs) kennen, einschließlich deren Erstellung, Anzeige, Änderung und Löschung.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine neue ACL erstellen	`vserver cifs share access-control create`
ACLs anzeigen	`vserver cifs share access-control show`
Eine ACL ändern	`vserver cifs share access-control modify`
Eine ACL löschen	`vserver cifs share access-control delete`

Dateizugriff mithilfe von Dateiberechtigungen absichern

Erweiterte NTFS-Dateiberechtigungen mithilfe der Registerkarte „Windows-Sicherheit“ für ONTAP SMB SVMs konfigurieren

Standard-NTFS-Dateiberechtigungen für Dateien und Ordner lassen sich über die Registerkarte **Windows-Sicherheit** im Fenster „Windows-Eigenschaften“ konfigurieren.

Bevor Sie beginnen

Der Administrator, der diese Aufgabe ausführt, muss über ausreichende NTFS-Berechtigungen verfügen, um die Berechtigungen für die ausgewählten Objekte zu ändern.

Über diese Aufgabe

Die Konfiguration von NTFS-Dateiberechtigungen erfolgt auf einem Windows-Host durch Hinzufügen von Einträgen zu NTFS-Zugriffskontrolllisten (DACLs), die einem NTFS-Sicherheitsdeskriptor zugeordnet sind. Der Sicherheitsdeskriptor wird anschließend auf NTFS-Dateien und Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows-Benutzeroberfläche übernommen.

Schritte

1. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
2. Das Dialogfeld **Netzlaufwerk verbinden** ausfüllen:

   a. Einen Laufwerksbuchstaben auswählen.

   b. Geben Sie im Feld **Ordner** den Namen des CIFS-Servers ein, der die Freigabe enthält, die die Daten enthält, für die Berechtigungen angewendet werden sollen, sowie den Namen der Freigabe.

      Wenn der Name Ihres CIFS-Servers “CIFS_SERVER” ist und Ihre Freigabe “share1” heißt, sollte `\\CIFS_SERVER\share1` eingegeben werden.

      > Sie können die IP-Adresse der Datenschnittstelle für den CIFS-Server anstelle des CIFS-Servernamens angeben.

   c. Klicken Sie auf **Finish**.

   Das von Ihnen ausgewählte Laufwerk ist eingebunden und einsatzbereit, wobei das Windows Explorer-Fenster die in der Freigabe enthaltenen Dateien und Ordner anzeigt.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das NTFS-Dateiberechtigungen festgelegt werden sollen.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis und wählen Sie dann **Eigenschaften**.
5. Die Registerkarte **Sicherheit** auswählen.

   Die Registerkarte **Sicherheit** zeigt die Liste der Benutzer und Gruppen an, für die NTFS-Berechtigungen festgelegt sind. Das Feld **Berechtigungen für** zeigt eine Liste der für jeden ausgewählten Benutzer oder jede ausgewählte Gruppe geltenden Allow- und Deny-Berechtigungen an.

6. Auf **Erweitert** klicken.

   Das Fenster „Windows-Eigenschaften“ zeigt Informationen zu bestehenden Dateiberechtigungen an, die Benutzern und Gruppen zugewiesen sind.

7. **Berechtigungen ändern** auswählen.

   Das Berechtigungsfenster wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie möchten…	Führen Sie folgende Schritte aus…
Erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe festlegen	a. Klicken Sie auf **Add**. b. Im Feld **Geben Sie den Namen des auszuwählenden Objekts ein** den Namen des Benutzers oder der Gruppe eingeben, die hinzugefügt werden soll. c. Klicken Sie auf **OK**.
Erweiterte NTFS-Berechtigungen eines Benutzers oder einer Gruppe ändern	a. Im Feld **Berechtigungseinträge:** den Benutzer oder die Gruppe auswählen, deren erweiterte Berechtigungen geändert werden sollen. b. Klicken Sie auf **Bearbeiten**.
Erweiterte NTFS-Berechtigungen für einen Benutzer oder eine Gruppe entfernen	a. Im Feld **Berechtigungseinträge:** den Benutzer oder die Gruppe auswählen, die entfernt werden soll. b. Klicken Sie auf **Entfernen**. c. Weiter zu Schritt 13.

   Wenn erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe hinzugefügt oder die erweiterten NTFS-Berechtigungen für einen bestehenden Benutzer oder eine bestehende Gruppe geändert werden, öffnet sich das Dialogfeld „Berechtigungseintrag für <Object>“.

9. Im Feld **Anwenden auf** kann ausgewählt werden, wie dieser NTFS-Dateiberechtigungseintrag angewendet werden soll.

   Wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei einrichten, ist das Feld **Anwenden auf** nicht aktiv. Die Einstellung **Anwenden auf** ist standardmäßig auf **Nur dieses Objekt** festgelegt.

10. Im Feld **Berechtigungen** werden die Kontrollkästchen **Zulassen** oder **Verweigern** für die erweiterten Berechtigungen ausgewählt, die auf dieses Objekt angewendet werden sollen.

    - Um den angegebenen Zugriff zuzulassen, das Kontrollkästchen **Zulassen** auswählen.
    - Um den angegebenen Zugriff nicht zuzulassen, das Kontrollkästchen **Verweigern** auswählen. Berechtigungen können für die folgenden erweiterten Rechte festgelegt werden:
    - **Volle Kontrolle**

      Wenn diese erweiterte Berechtigung ausgewählt wird, werden alle anderen erweiterten Berechtigungen automatisch ausgewählt (entweder „Erlauben“ oder „Verweigern“).

    - **Ordner durchsuchen / Datei ausführen**
    - **Ordner auflisten / Daten lesen**
    - **Attribute lesen**
    - **Erweiterte Attribute lesen**

- **Dateien erstellen / Daten schreiben**
- **Ordner erstellen / Daten anhängen**
- **Attribute schreiben**
- **Erweiterte Attribute schreiben**
- **Unterordner und Dateien löschen**
- **Löschen**
- **Leseberechtigungen**
- **Berechtigungen ändern**
- **Verantwortung übernehmen**

> Falls einzelne Kontrollkästchen für erweiterte Berechtigungen nicht auswählbar sind, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt geerbt werden.

11. Wenn Unterordner und Dateien dieses Objekts diese Berechtigungen erben sollen, aktivieren Sie das Kontrollkästchen **Diese Berechtigungen nur auf Objekte und/oder Container innerhalb dieses Containers anwenden**.
12. Klicken Sie auf **OK**.
13. Nachdem das Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen abgeschlossen ist, wird die Vererbungseinstellung für dieses Objekt festgelegt:
    - Das Kontrollkästchen **Vererbbare Berechtigungen vom übergeordneten Objekt einbeziehen** auswählen.

      Dies ist die Standardeinstellung.
    - Das Kontrollkästchen **Alle Berechtigungen von untergeordneten Objekten durch von diesem Objekt vererbbare Berechtigungen ersetzen** auswählen.

      Diese Einstellung ist im Dialogfeld „Berechtigungen“ nicht vorhanden, wenn NTFS-Dateiberechtigungen für eine einzelne Datei festgelegt werden.

      > Seien Sie bei der Auswahl dieser Einstellung vorsichtig. Diese Einstellung entfernt alle vorhandenen Berechtigungen auf allen untergeordneten Objekten und ersetzt sie durch die Berechtigungseinstellungen dieses Objekts. Es könnten versehentlich Berechtigungen entfernt werden, die nicht entfernt werden sollten. Dies ist besonders relevant beim Festlegen von Berechtigungen in einem Volume oder qtree mit gemischtem Sicherheitsstil. Wenn untergeordnete Objekte einen effektiven UNIX-Sicherheitsstil aufweisen, führt das Übertragen von NTFS-Berechtigungen auf diese untergeordneten Objekte dazu, dass ONTAP diese Objekte vom UNIX-Sicherheitsstil in den NTFS-Sicherheitsstil ändert und alle UNIX-Berechtigungen auf diesen untergeordneten Objekten durch NTFS-Berechtigungen ersetzt werden.
    - Wählen Sie beide Kästchen aus.
    - Keines der Kästchen wird ausgewählt.
14. Klicken Sie auf **OK**, um das Fenster **Berechtigungen** zu schließen.
15. Klicken Sie auf **OK**, um das Fenster **Erweiterte Sicherheitseinstellungen für <Object>** zu schließen.

Weitere Informationen zum Festlegen erweiterter NTFS-Berechtigungen enthält die Windows-

Dokumentation.

Verwandte Informationen

- NTFS-Sicherheitsdeskriptoren auf Servern erstellen
- Informationen zur Dateisicherheit auf NTFS Security-Style-Volumes
- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

ONTAP Befehle für SMB NTFS-Dateiberechtigungen

NTFS-Dateiberechtigungen für Dateien und Verzeichnisse lassen sich mithilfe der ONTAP-Befehlszeilenschnittstelle konfigurieren. Dies ermöglicht die Konfiguration von NTFS-Dateiberechtigungen, ohne dass eine Verbindung zu den Daten über eine SMB-Freigabe auf einem Windows-Client erforderlich ist.

Sie können NTFS-Dateiberechtigungen konfigurieren, indem Sie Einträge zu den NTFS-Zugriffskontrolllisten (DACLs) hinzufügen, die einem NTFS-Sicherheitsdeskriptor zugeordnet sind. Der Sicherheitsdeskriptor wird anschließend auf NTFS-Dateien und Verzeichnisse angewendet.

NTFS-Dateiberechtigungen können nur über die Befehlszeile konfiguriert werden. NFSv4-ACLs können über die Befehlszeile nicht konfiguriert werden.

Schritte

1. Ein NTFS-Sicherheitsdeskriptor wird erstellt.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. DACLs zum NTFS-Sicherheitsdeskriptor hinzufügen.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Eine Datei-/Verzeichnissicherheitsrichtlinie erstellen.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

UNIX-Dateiberechtigungen bieten Zugriffskontrolle beim Zugriff auf Dateien über ONTAP SMB-Server.

Ein FlexVol volume kann einen von drei Sicherheitsstilen aufweisen: NTFS, UNIX oder gemischt. Der Zugriff auf Daten über SMB ist unabhängig vom Sicherheitsstil möglich; für den Zugriff auf Daten mit effektiver UNIX-Sicherheit sind jedoch entsprechende UNIX-Dateiberechtigungen erforderlich.

Beim Datenzugriff über SMB kommen verschiedene Zugriffskontrollen zum Einsatz, um festzustellen, ob ein Benutzer zur Ausführung einer angeforderten Aktion berechtigt ist:

- Exportberechtigungen

  Die Konfiguration von Exportberechtigungen für den SMB-Zugriff ist optional.

- Freigabeberechtigungen
- Dateiberechtigungen

  Folgende Arten von Dateiberechtigungen können für die Daten angewendet werden, auf denen der Benutzer eine Aktion ausführen möchte:

  - NTFS
  - UNIX NFSv4-ACLs
  - UNIX-Modusbits

Für Daten mit NFSv4-ACLs oder gesetzten UNIX-Modusbits werden UNIX-Style-Berechtigungen verwendet, um die Dateizugriffsrechte auf die Daten zu bestimmen. Der SVM-Administrator muss die entsprechenden Dateiberechtigungen festlegen, damit Benutzer die Rechte haben, die gewünschte Aktion durchzuführen.

> Daten in einem Volume mit gemischtem Sicherheitsstil können entweder den effektiven Sicherheitsstil NTFS oder UNIX aufweisen. Wenn die Daten den effektiven UNIX-Sicherheitsstil haben, werden NFSv4-Berechtigungen oder UNIX-Modusbits verwendet, um die Dateizugriffsrechte für die Daten zu bestimmen.

Sicherer Dateizugriff durch Dynamic Access Control (DAC)

Informationen zur DAC-Dateizugriffsicherheit für ONTAP SMB-Server

Sie können den Zugriff sichern, indem Sie die dynamische Zugriffssteuerung nutzen und zentrale Zugriffsrichtlinien in Active Directory erstellen und diese über angewendete Gruppenrichtlinienobjekte (GPOs) auf Dateien und Ordner auf SVMs anwenden. Es besteht die Möglichkeit, die Protokollierung so zu konfigurieren, dass zentrale Zugriffsrichtlinien-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen an zentralen Zugriffsrichtlinien zu sehen, bevor diese angewendet werden.

Ergänzungen zu den CIFS-Anmeldeinformationen

Vor der dynamischen Zugriffssteuerung enthielt eine CIFS-Anmeldeinformation die Identität des Sicherheitsprinzipals (des Benutzers) und die Windows-Gruppenzugehörigkeit. Mit der dynamischen Zugriffssteuerung werden der Anmeldeinformation drei weitere Informationstypen hinzugefügt: Geräteidentität, Geräteansprüche und Benutzeransprüche.

- Geräteidentität

  Das Analogon zu den Identitätsinformationen des Benutzers, nur dass es sich um die Identität und Gruppenzugehörigkeit des Geräts handelt, von dem sich der Benutzer einloggt.

- Geräteansprüche

  Aussagen über einen Gerätesicherheitsprinzipal. Beispielsweise könnte eine Geräteaussage lauten, dass das Gerät Mitglied einer bestimmten Organisationseinheit (OU) ist.

- Benutzeransprüche

  Aussagen über einen Benutzer-Sicherheitsprinzipal. Beispielsweise könnte eine Benutzer-Assertion lauten, dass das AD-Konto Mitglied einer bestimmten OU ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Organisationen, Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzeransprüchen, Geräteansprüchen und Ressourceneigenschaften enthalten, zentral bereitzustellen und zu verwalten.

Beispielsweise muss ein Benutzer, um auf geschäftskritische Daten zuzugreifen, Vollzeitbeschäftigter sein und darf nur von einem verwalteten Gerät aus auf die Daten zugreifen. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus an Dateiserver verteilt.

Zentrale Bereitstellung von Zugriffsrichtlinien mit erweiterter Protokollierung

Zentrale Zugriffsrichtlinien können „staged“ werden, wobei sie bei Dateizugriffsprüfungen in einer „what-if“-Manier ausgewertet werden. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam gewesen wäre, und wie sich das von der aktuellen Konfiguration unterscheidet, werden als Protokollierungsereignis erfasst. Auf diese Weise können Administratoren Protokollierungsereignisse nutzen, um die Auswirkungen einer Änderung der Zugriffsrichtlinie zu untersuchen, bevor die Richtlinie tatsächlich angewendet wird. Nach der Bewertung der Auswirkungen einer Änderung der Zugriffsrichtlinie kann die Richtlinie über GPOs auf die gewünschten SVMs bereitgestellt werden.

Verwandte Informationen

- Informationen zu unterstützten Gruppenrichtlinienobjekten (GPOs)
- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- GPO-Unterstützung auf Servern aktivieren oder deaktivieren
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.
- Informationen zur Serversicherheit
- "SMB und NFS Auditierung und Sicherheitsverfolgung"

Unterstützte DAC-Funktionalität für ONTAP SMB Server

Wenn Sie Dynamic Access Control (DAC) auf Ihrem CIFS-Server verwenden möchten, ist es wichtig zu verstehen, wie ONTAP die Dynamic Access Control Funktionalität in Active Directory-Umgebungen unterstützt.

Unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Ansprüche im Dateisystem	Ansprüche sind einfache Namens-Wert-Paare, die eine bestimmte Wahrheit über einen Benutzer aussagen. Benutzeranmeldeinformationen enthalten Anspruchsinformationen, und Sicherheitsdeskriptoren von Dateien können Zugriffsprüfungen durchführen, die auch Anspruchsprüfungen umfassen. Dies gibt Administratoren eine feinere Kontrolle darüber, wer auf Dateien zugreifen kann.
Bedingte Ausdrücke für Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer dem Sicherheitsdeskriptor der Datei beliebig komplexe bedingte Ausdrücke hinzufügen. Der bedingte Ausdruck kann Prüfungen auf Claims enthalten.
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art Zugriffskontrollliste (ACL), die in Active Directory gespeichert und einer Datei zugeordnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn sowohl die Zugriffsprüfungen des Sicherheitsdeskriptors auf dem Datenträger als auch die zugeordnete zentrale Zugriffsrichtlinie den Zugriff erlauben. Dies ermöglicht Administratoren, den Zugriff auf Dateien zentral (in Active Directory) zu steuern, ohne den Sicherheitsdeskriptor auf dem Datenträger ändern zu müssen.
Staging der zentralen Zugriffsrichtlinie	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinflussen, indem eine Änderung an den zentralen Zugriffsrichtlinien „gestagt“ wird und die Auswirkung der Änderung in einem Prüfbericht angezeigt wird.
Unterstützung für die Anzeige von Informationen zur zentralen Zugriffsrichtliniensicherheit mithilfe der ONTAP CLI	Erweitert den `vserver security file-directory show` Befehl, um Informationen über angewendete zentrale Zugriffsrichtlinien anzuzeigen.
Sicherheitsverfolgung einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace`Befehlsfamilie und zeigt Ergebnisse an, die Informationen über angewendete zentrale Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität nicht, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows-Dateiklassifizierungsinfrastruktur, die in ONTAP nicht unterstützt wird.
Erweiterte Überwachung mit Ausnahme des Stagings von zentralen Zugriffsrichtlinien	Nur das zentrale Staging von Zugriffsrichtlinien wird für erweiterte Prüfverfahren unterstützt.

Informationen zur Verwendung von DAC und zentralen Zugriffsrichtlinien mit ONTAP SMB-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien zum Schutz von Dateien und Ordnern auf CIFS-Servern sind bestimmte Aspekte zu berücksichtigen.

Der NFS-Zugriff kann dem Root-Benutzer verweigert werden, wenn eine Richtlinienregel für den Benutzer „domain\administrator“ gilt.

Unter bestimmten Umständen kann der NFS-Zugriff auf Root verweigert werden, wenn auf die Daten, auf die der Root-Benutzer zugreifen möchte, eine zentrale Zugriffsrichtlinie angewendet wird. Das Problem tritt auf, wenn die zentrale Zugriffsrichtlinie eine Regel enthält, die auf domain\administrator angewendet wird und das Root-Konto dem domain\administrator-Konto zugeordnet ist.

Anstatt die Regel auf den Benutzer domain\administrator anzuwenden, sollte die Regel auf eine Gruppe mit administrativen Rechten angewendet werden, wie zum Beispiel die domain\administrators Gruppe. Auf diese Weise kann root dem domain\administrator Konto zugeordnet werden, ohne dass root von diesem Problem betroffen ist.

Die Gruppe BUILTIN\Administrators des CIFS-Servers hat Zugriff auf Ressourcen, wenn die angewendete zentrale Zugriffsrichtlinie in Active Directory nicht gefunden wird.

Es ist möglich, dass auf Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien angewendet werden. Wenn der CIFS-Server versucht, mithilfe der SID der zentralen Zugriffsrichtlinie Informationen aus Active Directory abzurufen, stimmt die SID mit keiner vorhandenen SID einer zentralen Zugriffsrichtlinie in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standardwiederherstellungsrichtlinie für diese Ressource an.

Die lokale Standardwiederherstellungsrichtlinie gewährt der Gruppe BUILTIN\Administrators des CIFS-Servers Zugriff auf diese Ressource.

DAC für ONTAP SMB-Server aktivieren oder deaktivieren

Die Option, mit der Sie Dynamic Access Control (DAC) zum Schutz von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Die Option muss aktiviert werden, wenn Dynamic Access Control auf dem CIFS-Server verwendet werden soll. Falls später entschieden wird, Dynamic Access Control nicht mehr zum Schutz von auf dem CIFS-Server gespeicherten Objekten zu verwenden, kann die Option deaktiviert werden.

Informationen darüber, wie die dynamische Zugriffssteuerung in Active Directory konfiguriert wird, sind in der Microsoft TechNet Library zu finden.

"Microsoft TechNet: Übersicht über Szenarien zur dynamischen Zugriffskontrolle"

Über diese Aufgabe

Sobald die dynamische Zugriffskontrolle aktiviert ist, kann das Dateisystem ACLs mit Einträgen zur dynamischen Zugriffskontrolle enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge zur dynamischen Zugriffskontrolle ignoriert und neue werden nicht zugelassen.

Diese Option ist nur auf der Stufe „Erweitert“ verfügbar.

Schritt

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die Dynamic Access Control…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.

Verwaltung von ACLs mit DAC-ACEs, wenn DAC auf ONTAP SMB-Servern deaktiviert ist

Wenn Sie Ressourcen haben, auf die ACLs mit Dynamic Access Control ACEs angewendet wurden, und Sie Dynamic Access Control auf der Storage Virtual Machine (SVM) deaktivieren, müssen Sie die Dynamic Access Control ACEs entfernen, bevor Sie die nicht-Dynamic Access Control ACEs auf dieser Ressource verwalten können.

Über diese Aufgabe

Nachdem die dynamische Zugriffskontrolle deaktiviert ist, können bestehende nicht-dynamische Zugriffskontroll-ACEs weder entfernt noch neue nicht-dynamische Zugriffskontroll-ACEs hinzugefügt werden, bis die bestehenden dynamischen Zugriffskontroll-ACEs entfernt wurden.

Sie können das Tool, das Sie normalerweise zur Verwaltung von ACLs verwenden, für diese Schritte einsetzen.

Schritte

1. Ermitteln, welche Dynamic Access Control ACEs auf die Ressource angewendet sind.
2. Die ACEs der dynamischen Zugriffssteuerung aus der Ressource entfernen.
3. Nicht-dynamische Zugriffskontroll-ACEs können nach Bedarf zur Ressource hinzugefügt oder daraus entfernt werden.

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf ONTAP SMB Servern zu schützen

Es sind mehrere Schritte erforderlich, um den Zugriff auf Daten auf dem CIFS-Server mithilfe zentraler Zugriffsrichtlinien zu sichern, darunter das Aktivieren der Dynamic Access Control (DAC) auf dem CIFS-Server, das Konfigurieren zentraler Zugriffsrichtlinien in Active Directory, das Anwenden der zentralen Zugriffsrichtlinien auf Active Directory Container mit Gruppenrichtlinienobjekten (GPOs) und das Aktivieren von GPOs auf dem CIFS-Server.

Bevor Sie beginnen

- Das Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.

- Sie benötigen ausreichende Zugriffsrechte auf den Active Directory Domänencontrollern, um zentrale Zugriffsrichtlinien zu erstellen und GPOs auf die Container zu erstellen und anzuwenden, die die CIFS-Server enthalten.
- Sie benötigen ausreichende administrative Zugriffsrechte auf der Storage Virtual Machine (SVM), um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (GPOs) in Active Directory angewendet. Informationen zur Konfiguration zentraler Zugriffsrichtlinien in Active Directory sind in der Microsoft TechNet Library verfügbar.

"Microsoft TechNet: Szenario für zentrale Zugriffsrichtlinie"

Schritte

1. Die dynamische Zugriffskontrolle auf der SVM kann aktiviert werden, falls sie noch nicht aktiviert ist, indem der `vserver cifs options modify` Befehl verwendet wird.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Gruppenrichtlinienobjekte (GPOs) auf dem CIFS-Server können aktiviert werden, falls sie noch nicht aktiviert sind, indem der `vserver cifs group-policy modify` Befehl verwendet wird.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien in Active Directory erstellen.
4. Ein Gruppenrichtlinienobjekt (GPO) wird erstellt, um die zentralen Zugriffsrichtlinien auf Active Directory bereitzustellen.
5. Die Gruppenrichtlinie wird auf den Container angewendet, in dem sich das Computerkonto des CIFS-Servers befindet.
6. Die auf den CIFS-Server angewendeten GPOs werden mit dem `vserver cifs group-policy update` Befehl manuell aktualisiert.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Es sollte überprüft werden, ob die zentrale Zugriffsrichtlinie des Gruppenrichtlinienobjekts (GPO) auf die Ressourcen auf dem CIFS-Server angewendet wird, indem der `vserver cifs group-policy show-applied` Befehl verwendet wird.

   Das folgende Beispiel zeigt, dass die Default Domain Policy zwei zentrale Zugriffsrichtlinien enthält, die auf den CIFS-Server angewendet werden:

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   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
2 entries were displayed.
```

Verwandte Informationen

- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- DAC für Server aktivieren oder deaktivieren

Informationen zur DAC-Sicherheit für ONTAP SMB-Server

Sie können Informationen zur dynamischen Zugriffssteuerung (DAC) auf NTFS-Volumes und zu Daten mit effektiver NTFS-Sicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen. Dies umfasst Informationen zu bedingten ACEs, Ressourcen-ACEs und

zentralen Zugriffsrichtlinien-ACEs. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Wo die Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Informationen zur Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, bei denen die hexadezimale Bitmaske in ein Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Das folgende Beispiel zeigt Sicherheitsinformationen zur Dynamic Access Control über den Pfad `/vol1` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
               File Inode Number: 112
                  Security Style: mixed
                 Effective Style: ntfs
                  DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attribute: -
                    Unix User Id: 0
                   Unix Group Id: 1
                  Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
                            ACLs: NTFS Security Descriptor
                                  Control:0xbf14
                                  Owner:CIFS1\Administrator
```

```
                                        Group:CIFS1\Domain Admins
                                        SACL - ACEs
                                           ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                           RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                           POLICY ID-All resources - No Write-
0x0-OI|CI
                                        DACL - ACEs
                                           ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                           ALLOW-Everyone-0x1f01ff-OI|CI
                                           ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Verwandte Informationen

- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln

Überlegungen zum Zurücksetzen von DAC auf ONTAP SMB-Servern

Sie sollten sich darüber im Klaren sein, was passiert, wenn auf eine Version von ONTAP zurückgesetzt wird, die Dynamic Access Control (DAC) nicht unterstützt, und was vor und nach dem Zurücksetzen zu tun ist.

Wenn der Cluster auf eine Version von ONTAP zurückgesetzt werden soll, die Dynamic Access Control nicht unterstützt, und Dynamic Access Control auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert ist, sind vor dem Zurücksetzen die folgenden Schritte erforderlich:

- Die dynamische Zugriffskontrolle muss auf allen SVMs deaktiviert werden, auf denen sie im Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster, die den `cap-staging` Ereignistyp enthalten, so ändern, dass nur der `file-op` Ereignistyp verwendet wird.

Einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control-ACEs sollten verstanden und berücksichtigt werden:

- Wenn der Cluster zurückgesetzt wird, werden bestehende Dynamic Access Control ACEs nicht entfernt; sie werden jedoch bei Dateizugriff-Prüfungen ignoriert.
- Da Dynamic Access Control-ACEs nach der Rücksetzung ignoriert werden, ändert sich der Zugriff auf Dateien mit Dynamic Access Control-ACEs.

  Dies könnte dazu führen, dass Benutzer auf Dateien zugreifen können, auf die sie zuvor keinen Zugriff hatten, oder umgekehrt, dass sie auf Dateien nicht mehr zugreifen können, auf die sie zuvor Zugriff hatten.

- Nicht-dynamische Zugriffskontroll-ACEs sollten auf die betroffenen Dateien angewendet werden, um deren vorheriges Sicherheitsniveau wiederherzustellen.

  Dies kann entweder vor dem Zurücksetzen oder unmittelbar nach Abschluss der Rücksetzung erfolgen.

> Da Dynamic Access Control-ACEs nach dem Zurücksetzen ignoriert werden, ist es nicht erforderlich, sie zu entfernen, wenn nicht-Dynamic Access Control-ACEs auf die betroffenen Dateien angewendet werden. Falls gewünscht, können sie manuell entfernt werden.

SMB-Zugriff mithilfe von Exportrichtlinien absichern

Informationen zur Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff

Wenn auf dem SMB-Server Exportregeln für den SMB-Zugriff aktiviert sind, werden Exportregeln verwendet, um den Zugriff von SMB-Clients auf SVM-Volumes zu steuern. Für den Datenzugriff kann eine Exportregel erstellt werden, die den SMB-Zugriff erlaubt, und anschließend der Richtlinie die Volumes zugeordnet werden, die SMB-Freigaben enthalten.

Für eine Exportregel gilt eine oder mehrere Regeln, die festlegen, welche Clients Zugriff auf die Daten erhalten und welche Authentifizierungsprotokolle für Lese- und Schreibzugriff unterstützt werden. Exportregeln können so konfiguriert werden, dass der Zugriff über SMB für alle Clients, ein Subnetz von Clients oder einen bestimmten Client erlaubt ist und dass die Authentifizierung mittels Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung bei der Bestimmung des Lese- und Schreibzugriffs auf Daten zulässig ist.

Nach der Verarbeitung aller auf die Exportregel angewendeten Exportregeln kann ONTAP feststellen, ob dem Client Zugriff gewährt wird und welche Zugriffsebene gewährt wird. Exportregeln gelten für Client-Rechner, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen nicht die Windows-Benutzer- und -gruppenbasierte Authentifizierung und Autorisierung. Exportregeln bieten eine zusätzliche Sicherheitsebene zum Schutz des Zugriffs, zusätzlich zu den Berechtigungen für Freigaben und Dateizugriff.

Jedem Volume wird genau eine Exportregel zugeordnet, um den Clientzugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportregeln enthalten. Dadurch ergeben sich für SVMs mit mehreren Volumes folgende Möglichkeiten:

- Weisen Sie jedem Volume der SVM unterschiedliche Exportrichtlinien zu, um die Zugriffskontrolle für jeden einzelnen Client auf jedes Volume in der SVM zu ermöglichen.
- Dieselbe Exportregel kann mehreren Volumes der SVM zugewiesen werden, sodass eine identische Clientzugriffskontrolle möglich ist, ohne für jedes Volume eine neue Exportregel erstellen zu müssen.

Jede SVM verfügt über mindestens eine Export-Richtlinie namens „`default`“, die keine Regeln enthält. Sie können diese Export-Richtlinie nicht löschen, aber Sie können sie umbenennen oder ändern. Jedes Volume auf der SVM ist standardmäßig der Standard-Export-Richtlinie zugeordnet. Wenn Export-Richtlinien für den SMB-Zugriff auf der SVM deaktiviert sind, hat die Export-Richtlinie „`default`“ keine Auswirkungen auf den SMB-Zugriff.

Es ist möglich, Regeln zu konfigurieren, die sowohl NFS- als auch SMB-Hosts Zugriff gewähren, und diese Regel mit einer Exportregel zu verknüpfen, die anschließend dem Volume zugeordnet werden kann, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Alternativ kann für einige Volumes, auf die nur SMB-Clients zugreifen müssen, eine Exportregel mit Regeln konfiguriert werden, die ausschließlich den Zugriff über das SMB-Protokoll erlauben und für die Authentifizierung bei Lese- und Schreibzugriffen

ausschließlich Kerberos oder NTLM (oder beides) verwenden. Die Exportregel wird dann den Volumes zugeordnet, bei denen ausschließlich SMB-Zugriff erforderlich ist.

Wenn Exportregeln für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportregel nicht zugelassen wird, schlägt die Anfrage mit einer „Zugriff verweigert“-Meldung fehl. Wenn ein Client keiner Regel in der Exportregel des Volumes entspricht, wird der Zugriff verweigert. Ist eine Exportregel leer, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen den Zugriff ansonsten erlauben würden. Das bedeutet, dass die Exportregel auf Volumes mit SMB-Freigaben mindestens Folgendes zulassen muss:

- Zugriff für alle Clients oder die entsprechende Teilmenge der Clients zulassen
- Zugriff über SMB zulassen
- Angemessener Lese- und Schreibzugriff durch Kerberos- oder NTLM-Authentifizierung (oder beides) möglich

Informationen dazu "Konfiguration und Verwaltung von Exportrichtlinien".

Informationen zu ONTAP SMB Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportregel. Exportregeln gleichen Clientzugriffsanfragen an ein Volume mit spezifischen, von Ihnen konfigurierten Parametern ab, um festzulegen, wie die Clientzugriffsanfragen behandelt werden.

Eine Exportregel muss mindestens in einer Exportregel enthalten sein, damit Clients Zugriff erhalten. Wenn eine Exportregel mehr als eine Regel enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportregel erscheinen. Die Reihenfolge der Regeln wird durch die Regelindexnummer bestimmt. Wenn eine Regel auf einen Client zutrifft, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Wenn keine Regel zutrifft, wird dem Client der Zugriff verweigert.

Exportregeln können so konfiguriert werden, dass die Clientzugriffsberechtigungen anhand der folgenden Kriterien bestimmt werden:

- Das vom Client, der die Anfrage sendet, verwendete Protokoll für den Dateizugriff, beispielsweise NFSv4 oder SMB.
- Eine Client-Kennung, zum Beispiel Hostname oder IP-Adresse.

  Die maximale Größe des `-clientmatch` Feldes beträgt 4096 Zeichen.

- Der vom Client zur Authentifizierung verwendete Sicherheitstyp, beispielsweise Kerberos v5, NTLM oder AUTH_SYS.

Wenn eine Regel mehrere Kriterien festlegt, muss der Client alle erfüllen, damit die Regel Anwendung findet.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv3-Protokoll gesendet und der Client hat die IP-Adresse 10.1.17.37.

Obwohl das Client-Zugriffsprotokoll übereinstimmt, befindet sich die IP-Adresse des Clients in einem anderen Subnetz als dem in der Exportregel angegebenen. Daher schlägt die Clientzuordnung fehl und diese Regel gilt für diesen Client nicht.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv4-Protokoll gesendet und der Client hat die IP-Adresse 10.1.16.54.

Das Protokoll für den Dateizugriff stimmt überein und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientübereinstimmung erfolgreich und diese Regel gilt für diesen Client. Der Client erhält unabhängig von seinem Sicherheitstyp lesen/schreiben-Zugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und hat sich mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich mit AUTH_SYS authentifiziert.

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients Lesezugriff, unabhängig vom Sicherheitstyp, mit dem sie sich authentifiziert haben. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese- und Schreibzugriff, da er sich mit dem genehmigten Sicherheitstyp Kerberos v5 authentifiziert hat. Client #2 erhält keinen Lese- und Schreibzugriff.

Beispiele für ONTAP Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen

Die Beispiele zeigen, wie Exportrichtlinienregeln erstellt werden, die den Zugriff über SMB auf einer SVM einschränken oder zulassen, auf der Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für den SMB-Zugriff sind standardmäßig deaktiviert. Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen, sind nur zu konfigurieren, wenn Exportrichtlinien für den SMB-Zugriff aktiviert wurden.

Exportregel nur für SMB-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: cifs1
- Indexnummer: 1
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Für Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese- und Schreibzugriff: Für Clients mit Kerberos-Authentifizierung

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Exportregel für SMB- und NFS-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM namens "vs1", die die folgende Konfiguration aufweist:

- Richtlinienname: cifsnfs1
- Indexnummer: 2
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: SMB und NFS-Zugriff
- Nur-Lese-Zugriff: Für alle Clients
- Lese- und Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zuordnung zur Benutzer-ID 65534 (die typischerweise dem Benutzernamen nobody zugeordnet ist)
- SUID- und SGID-Zugriff: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch
192.168.1.0/255.255.255.0 -rorule any -rwrule krb5,ntlm -anon 65534 -allow
-suid true
```

Exportregel für SMB-Zugriff ausschließlich über NTLM

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: ntlm1
- Indexnummer: 1

- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden
- Lese- und Schreibzugriff: Nur für Clients, die NTLM verwenden

> Wenn Sie die Option „Nur lesen“ oder „Lesen/Schreiben“ für den NTLM-only-Zugriff konfigurieren, müssen Sie IP-adressbasierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies ist darauf zurückzuführen, dass ONTAP bei Verwendung eines Hostnamens zur Überprüfung der Zugriffsrechte des Clients Kerberos Service Principal Names (SPN) verwendet. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule ntlm -rwrule ntlm
```

ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren

Sie können Exportrichtlinien für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Verwendung von Exportrichtlinien zur Steuerung des SMB-Zugriffs auf Ressourcen ist optional.

Bevor Sie beginnen

Die folgenden Voraussetzungen gelten für die Aktivierung von Exportrichtlinien für SMB:

- Der Client muss über einen "PTR"-Eintrag im DNS verfügen, bevor die Exportregeln für diesen Client erstellt werden.
- Ein zusätzlicher Satz von „A“- und „PTR“-Einträgen für Hostnamen ist erforderlich, wenn die SVM Zugriff auf NFS-Clients bereitstellt und der Hostname, der für den NFS-Zugriff verwendet werden soll, sich vom CIFS-Servernamen unterscheidet.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für den SMB-Zugriff standardmäßig deaktiviert. Exportrichtlinien für den SMB-Zugriff können aktiviert werden, wenn der Zugriff basierend auf Authentifizierungsprotokoll, Client-IP-Adressen oder Hostnamen gesteuert werden soll. Exportrichtlinien für den SMB-Zugriff können jederzeit aktiviert oder deaktiviert werden.

> Durch die Aktivierung von Exportrichtlinien für CIFS/SMB in einer NFS-fähigen SVM kann ein Linux-Client den `showmount -e` Befehl auf der SVM verwenden, um die Verbindungspfade aller SMB-Volumes mit zugehörigen Exportrichtlinienregeln anzuzeigen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Exportrichtlinien aktivieren oder deaktivieren:
   - Exportrichtlinien aktivieren: `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`

- Exportrichtlinien deaktivieren: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht die Verwendung von Exportrichtlinien zur Steuerung des SMB-Clientzugriffs auf Ressourcen auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Die SMB-Exportregel des ONTAP SVM-Root-Volumes öffnen

Wenn Sie SMB-Exportrichtlinienregeln aktiviert haben, muss die Standardexportrichtlinie des SVM-Root-Volumes eine Regel enthalten, die allen Clients offenen Zugriff über SMB erlaubt. Ohne eine solche Regel wird allen SMB-Clients der Zugriff auf die SVM und ihre Volumes verweigert. Exportrichtlinienregeln sind standardmäßig deaktiviert.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine Standard-Exportregel (genannt default) für das Root-Volume der SVM erstellt. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können.

Es empfiehlt sich zu überprüfen, ob der gesamte SMB-Zugriff in der Standard-Exportregel offen ist, und den Zugriff auf einzelne Volumes später durch das Erstellen benutzerdefinierter Exportregeln für einzelne Volumes oder qtrees einzuschränken.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standard-Exportregel für das Root-Volume: `vserver export-policy rule show`

   Die Ausgabe des Befehls sollte in etwa wie folgt aussehen:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                Vserver: vs1.example.com
                            Policy Name: default
                             Rule Index: 1
                        Access Protocol: cifs
```

```
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                            RO Access Rule: any
                            RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: any
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Existiert eine solche Regel, die offenen Zugang erlaubt, ist diese Aufgabe abgeschlossen. Falls nicht, folgt der nächste Schritt.

2. Eine Exportregel für das SVM-Root-Volume erstellen: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Die Regelerstellung kann mithilfe des `vserver export-policy rule show` Befehls überprüft werden.

Ergebnisse

Jeder SMB-Client kann nun auf jedes Volume oder jeden Qtree zugreifen, der auf der SVM erstellt wurde.

Verwandte Informationen

"Erfahren Sie, wie Sie ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren".

Sicherer Dateizugriff mit Storage Level Access Guard

Informationen zum sicheren ONTAP SMB Dateizugriff mit Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native Dateisicherheits- sowie Export- und Freigabesicherheitsmechanismen kann Storage-Level Access Guard konfiguriert werden, eine dritte Sicherheitsebene, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff aus allen NAS-Protokollen auf das Speicherobjekt, auf das sie angewendet wird.

Es werden ausschließlich NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP Sicherheitsprüfungen für UNIX-Benutzer beim Zugriff auf Daten auf Volumes durchführen kann, für die Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM zugeordnet sein, der das Volume besitzt.

Verhalten des Storage-Level Access Guard

- Storage-Level Access Guard gilt für alle Dateien oder alle Verzeichnisse in einem Storage-Objekt.

  Da alle Dateien oder Verzeichnisse in einem Volume den Einstellungen des Storage-Level Access Guard unterliegen, ist eine Vererbung durch Weitergabe nicht erforderlich.

- Storage-Level Access Guard kann so konfiguriert werden, dass es nur für Dateien, nur für Verzeichnisse oder sowohl für Dateien als auch für Verzeichnisse innerhalb eines Volumes gilt.
  - Datei- und Verzeichnissicherheit

    Gilt für jedes Verzeichnis und jede Datei innerhalb des Speicherobjekts. Dies ist die Standardeinstellung.

- Dateisicherheit

  Gilt für jede Datei innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Verzeichnissen aus.

- Verzeichnissicherheit

  Gilt für jedes Verzeichnis innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Dateien aus.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

- Wenn die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus angezeigt werden, ist die Storage-Level Access Guard Sicherheit nicht sichtbar.

  Sie wird auf Ebene des Speicherobjekts angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Die Sicherheit auf Storage-Ebene kann einem Client nicht entzogen werden, auch nicht von einem Systemadministrator (Windows oder UNIX).

  Es ist so konzipiert, dass es nur von Speicheradministratoren geändert werden kann.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS- oder gemischtem Sicherheitsstil anwenden.
- Sie können Storage-Level Access Guard auf Volumes mit UNIX-Sicherheitsstil anwenden, sofern auf der SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume Verbindungspfad gemountet werden und Storage-Level Access Guard auf diesem Pfad vorhanden ist, wird es nicht auf die darunter gemounteten Volumes übertragen.
- Der Storage-Level Access Guard Sicherheitsdeskriptor wird mit SnapMirror Datenreplizierung und mit SVM-Replikation repliziert.
- Für Virenscanner gelten Sonderregelungen.

  Diesen Servern wird ein Ausnahmezugriff zum Durchsuchen von Dateien und Verzeichnissen gewährt, selbst wenn Storage-Level Access Guard den Zugriff auf das Objekt verweigert.

- FPolicy-Benachrichtigungen werden nicht gesendet, wenn der Zugriff aufgrund von Storage-Level Access Guard verweigert wird.

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch die kombinierte Wirkung der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Storage-Level Access Guard-Berechtigungen und der nativ auf Dateien und/oder Verzeichnisse angewendeten Dateiberechtigungen bestimmt. Alle Sicherheitsebenen werden ausgewertet, um zu bestimmen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis hat. Die Sicherheitszugriffsprüfungen erfolgen in folgender Reihenfolge:

1. SMB-Freigabe- oder NFS-Export-Berechtigungen
2. Zugriffsschutz auf Storage-Ebene
3. NTFS-Datei-/Ordnerzugriffskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modusbits

Anwendungsfälle für den Einsatz von Storage-Level Access Guard

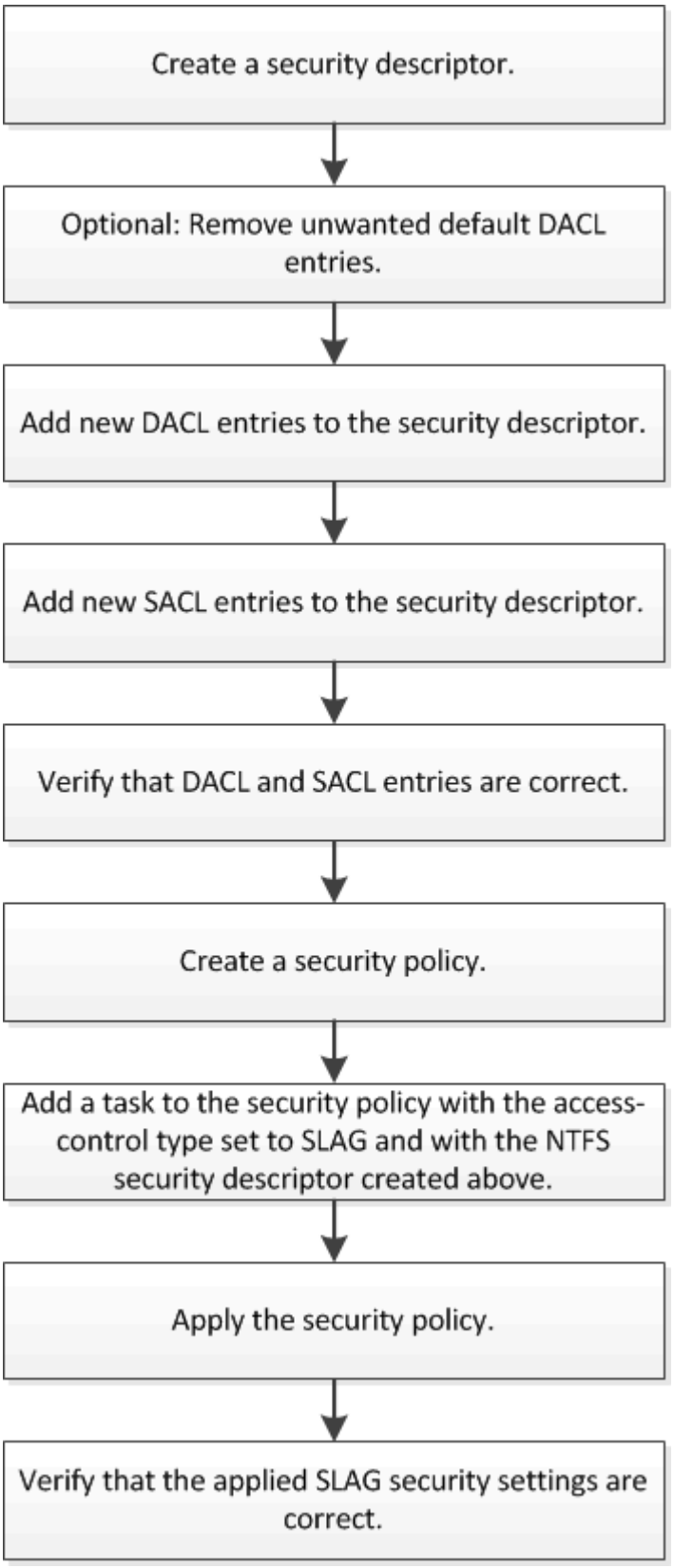
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Speicherebene, die für Clients nicht sichtbar ist, daher kann sie weder von Benutzern noch von Administratoren von ihren Desktops aus aufgehoben werden. In bestimmten Anwendungsfällen ist die Möglichkeit, den Zugriff auf Speicherebene zu steuern, von Vorteil.

Typische Anwendungsfälle für diese Funktion umfassen die folgenden Szenarien:

- Schutz des geistigen Eigentums durch Prüfung und Kontrolle aller Benutzerzugriffe auf Speicherebene
- Storage für Finanzdienstleistungsunternehmen, einschließlich Banken und Handelsgruppen
- Regierungsdienste mit separatem Dateispeicher für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB Servern

Der Workflow zur Konfiguration von Storage-Level Access Guard (SLAG) verwendet dieselben ONTAP CLI-Befehle wie die Konfiguration von NTFS-Dateiberechtigungen und Überwachungsrichtlinien. Statt den Datei- und Verzeichniszugriff auf einem bestimmten Ziel zu konfigurieren, wird SLAG auf dem entsprechenden Volume der Storage Virtual Machine (SVM) konfiguriert.



Verwandte Informationen

Storage Level Access Guard auf Servern konfigurieren

Storage-Level Access Guard auf ONTAP SMB-Servern konfigurieren

Es sind mehrere Schritte erforderlich, um Storage-Level Access Guard auf einem Volume oder Qtree zu konfigurieren. Storage-Level Access Guard bietet eine Zugriffssicherheit, die auf Speicherebene festgelegt wird. Sie bietet eine Sicherheit, die für alle Zugriffe aller NAS-Protokolle auf das Speicherobjekt gilt, auf das sie angewendet wurde.

Schritte

1. Ein Sicherheitsdeskriptor wird mithilfe des `vserver security file-directory ntfs create` Befehls erstellt.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Ein Sicherheitsdeskriptor wird mit den folgenden vier Standard-DACL-Zugriffskontrolleinträgen (ACEs) erstellt:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Wenn Sie bei der Konfiguration von Storage-Level Access Guard nicht die Standardeinträge verwenden möchten, können Sie diese entfernen, bevor Sie eigene ACEs erstellen und dem Sicherheitsdeskriptor hinzufügen.

2. Entfernen Sie alle standardmäßigen DACL-ACEs aus dem Sicherheitsdeskriptor, die nicht mit Storage-

Level Access Guard Sicherheit konfiguriert werden sollen:

a. Unerwünschte DACL-ACEs lassen sich mit dem `vserver security file-directory ntfs dacl remove` Befehl entfernen.

   In diesem Beispiel werden drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt: BUILTIN\Administrators, BUILTIN\Users und CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Es sollte überprüft werden, dass die DACL-ACEs, die nicht für die Storage-Level Access Guard Sicherheit verwendet werden sollen, mithilfe des `vserver security file-directory ntfs dacl show` Befehls aus dem Sicherheitsdeskriptor entfernt wurden.

   In diesem Beispiel bestätigt die Ausgabe des Befehls, dass drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt wurden, sodass nur noch der NT AUTHORITY\SYSTEM Standard-DACL-ACE-Eintrag übrig bleibt:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs dacl add` Befehl ein oder mehrere DACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei DACL-ACEs hinzugefügt:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs sacl add` Befehl ein oder mehrere SACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-ACEs hinzugefügt:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   ```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Es sollte überprüft werden, ob die DACL- und SACL-ACEs mithilfe der `vserver security file-directory ntfs dacl show`- und `vserver security file-directory ntfs sacl show` -Befehle jeweils korrekt konfiguriert sind.

   In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   In diesem Beispiel zeigt der folgende Befehl Informationen über SACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   ```

```
files
```

6. Eine Sicherheitsrichtlinie kann mithilfe des `vserver security file-directory policy create` Befehls erstellt werden.

   Das folgende Beispiel erstellt eine Richtlinie mit dem Namen “policy1”:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Es kann mithilfe des `vserver security file-directory policy show` Befehls überprüft werden, ob die Richtlinie korrekt konfiguriert ist.

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. Eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor wird zur Sicherheitsrichtlinie hinzugefügt, indem der `vserver security file-directory policy task add` Befehl mit dem `-access -control` Parameter, der auf `slag` gesetzt ist, verwendet wird.

   Eine Richtlinie kann zwar mehrere Storage-Level Access Guard Aufgaben enthalten, jedoch ist es nicht möglich, eine Richtlinie so zu konfigurieren, dass sie sowohl Datei-Verzeichnis- als auch Storage-Level Access Guard Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

   In diesem Beispiel wird der Richtlinie mit dem Namen „policy1“ eine Aufgabe hinzugefügt, die dem Sicherheitsdeskriptor „sd1“ zugewiesen ist. Sie ist dem `/datavol1` Pfad mit dem Zugriffskontrolltyp „slag“ zugeordnet.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Es kann überprüft werden, ob die Aufgabe korrekt konfiguriert ist, indem der `vserver security file-directory policy task show` Befehl verwendet wird.

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
   ```

```
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Die Sicherheitsrichtlinie „Storage-Level Access Guard“ wird mithilfe des `vserver security file-directory apply` Befehls angewendet.

    `vserver security file-directory apply -vserver vs1 -policy-name policy1`

    Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist terminiert.

11. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob die angewendeten Storage-Level Access Guard Sicherheitseinstellungen korrekt sind.

    In diesem Beispiel zeigt die Ausgabe des Befehls, dass die Storage-Level Access Guard-Sicherheit auf das NTFS-Volume angewendet wurde `/datavol1`. Auch wenn die standardmäßige DACL, die Vollzugriff für Everyone erlaubt, weiterhin besteht, beschränkt und protokolliert die Storage-Level Access Guard-Sicherheit den Zugriff auf die in den Storage-Level Access Guard-Einstellungen definierten Gruppen.

    `vserver security file-directory show -vserver vs1 -path /datavol1`

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
```

```
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-EXAMPLE\engineering-0x1f01ff
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                        SACL (Applies to Files):
                          AUDIT-EXAMPLE\Domain Users-0x120089-FA
                          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                        DACL (Applies to Files):
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-EXAMPLE\engineering-0x1f01ff
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Verwandte Informationen

- Befehle zur Verwaltung der NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und des Storage-Level Access Guard
- Konfigurationsworkflow für Storage-Level Access Guard auf Servern
- Informationen zu Storage-Level Access Guard auf Servern
- Storage-Level Access Guard auf Servern entfernen

Effektive SLAG-Matrix auf ONTAP SMB Servern

Sie können SLAG auf einem Volume, einem Qtree oder beiden konfigurieren. Die SLAG-Matrix definiert, auf welchem Volume oder Qtree die SLAG-Konfiguration in den verschiedenen, in der Tabelle aufgeführten Szenarien anwendbar ist.

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	k. A.	k. A.
Volumenzugriff in einer Snapshot	JA	NEIN	k. A.	k. A.
Qtree-Zugriff in einem AFS (wenn SLAG im Qtree vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn SLAG nicht im Qtree vorhanden ist)	JA	NEIN	NEIN	NEIN
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS vorhanden ist)	NEIN	NEIN	JA	NEIN

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS nicht vorhanden ist)	JA	NEIN	NEIN	NEIN

Informationen zu Storage-Level Access Guard auf ONTAP SMB-Servern

Storage-Level Access Guard ist eine dritte Sicherheitsebene, die auf ein Volume oder einen Qtree angewendet wird. Storage-Level Access Guard-Einstellungen können nicht über das Windows-Eigenschaftenfenster angezeigt werden. Zur Anzeige von Informationen zur Storage-Level Access Guard-Sicherheit, die zur Validierung der Konfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden können, ist die ONTAP CLI zu nutzen.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder Qtree angeben, dessen Storage-Level Access Guard Sicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

Schritt

1. Storage-Level Access Guard-Sicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Storage-Level Access Guard-Sicherheitsinformationen für das NTFS-Sicherheitsvolume mit dem Pfad `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
```

```
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Das folgende Beispiel zeigt die Storage-Level Access Guard-Informationen zum Volume mit gemischtem Sicherheitsstil am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Volumes hat effektive UNIX-Sicherheit. Das Volume verfügt über Storage-Level Access Guard-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
```

```
Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: Storage-Level Access Guard security
                        SACL (Applies to Directories):
                          AUDIT-EXAMPLE\Domain Users-0x120089-FA
                          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                        DACL (Applies to Directories):
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-EXAMPLE\engineering-0x1f01ff
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                        SACL (Applies to Files):
                          AUDIT-EXAMPLE\Domain Users-0x120089-FA
                          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                        DACL (Applies to Files):
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-EXAMPLE\engineering-0x1f01ff
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Storage-Level Access Guard auf ONTAP SMB-Servern entfernen

Sie können den Storage-Level Access Guard für ein Volume oder einen Qtree entfernen, wenn Sie die Zugriffssicherheit nicht mehr auf Storage-Level festlegen möchten. Das Entfernen des Storage-Level Access Guard ändert oder entfernt die reguläre NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob für das Volume oder den Qtree Storage-Level Access Guard konfiguriert ist.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

   ```
                     Vserver: vs1
                   File Path: /datavol2
         File Inode Number: 99
            Security Style: ntfs
           Effective Style: ntfs
            DOS Attributes: 10
    DOS Attributes in Text: ----D---
   Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0xbf14
                            Owner:BUILTIN\Administrators
                            Group:BUILTIN\Administrators
   ```

```
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                          Storage-Level Access Guard security
                          DACL (Applies to Directories):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                          DACL (Applies to Files):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Storage-Level Access Guard kann mit dem `vserver security file-directory remove-slag` Befehl entfernt werden.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Es kann mit dem `vserver security file-directory show` Befehl überprüft werden, ob Storage-Level Access Guard vom Volume oder Qtree entfernt wurde.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
```

```
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Dateizugriff mit SMB verwalten

Lokale Benutzer und Gruppen für Authentifizierung und Autorisierung verwenden

Informationen zu lokalen ONTAP SMB-Benutzern und -Gruppen

Es ist hilfreich, vor der Entscheidung, ob lokale Benutzer und Gruppen in Ihrer Umgebung konfiguriert und verwendet werden, zu wissen, was lokale Benutzer und Gruppen sind und einige grundlegende Informationen darüber zu kennen.

- **Lokaler Benutzer**

  Ein Benutzerkonto mit einer eindeutigen Sicherheitskennung (SID), das nur auf der Storage Virtual Machine (SVM) sichtbar ist, auf der es erstellt wurde. Lokale Benutzerkonten verfügen über eine Reihe von Attributen, darunter Benutzername und SID. Ein lokales Benutzerkonto authentifiziert sich lokal auf dem CIFS-Server mithilfe von NTLM-Authentifizierung.

  Benutzerkonten haben verschiedene Verwendungszwecke:

  - Wird verwendet, um einem Benutzer *User Rights Management*-Berechtigungen zu gewähren.
  - Dient zur Steuerung des Share-Level- und des Zugriffs auf Dateiebene auf Datei- und Ordnerressourcen, die sich im Besitz der SVM befinden.

- **Lokale Gruppe**

  Eine Gruppe mit einer eindeutigen SID ist nur auf der SVM sichtbar, auf der sie erstellt wurde. Gruppen enthalten eine Reihe von Mitgliedern. Mitglieder können lokale Benutzer, Domänenbenutzer, Domänengruppen und Domänencomputerkonten sein. Gruppen können erstellt, geändert oder gelöscht werden.

  Gruppen haben verschiedene Einsatzmöglichkeiten:

  - Wird verwendet, um Mitgliedern *User Rights Management*-Berechtigungen zu gewähren.
  - Dient zur Steuerung des Share-Level- und des Zugriffs auf Dateiebene auf Datei- und Ordnerressourcen, die sich im Besitz der SVM befinden.

- **Lokale Domäne**

  Eine Domäne mit lokalem Geltungsbereich, die durch die SVM begrenzt ist. Der Name der lokalen Domäne ist der CIFS-Servername. Lokale Benutzer und Gruppen sind innerhalb der lokalen Domäne enthalten.

- **Sicherheitskennung (SID)**

  Eine SID ist ein numerischer Wert variabler Länge, der Sicherheitsprinzipale im Windows-Stil identifiziert. Beispielsweise hat eine typische SID die folgende Form: S-1-5-21-3139654847-1303905135-2517279418-

123456.

- **NTLM-Authentifizierung**

  Eine Microsoft Windows-Sicherheitsmethode zur Authentifizierung von Benutzern auf einem CIFS-Server.

- **Cluster replizierte Datenbank (RDB)**

  Eine replizierte Datenbank mit einer Instanz auf jedem Knoten eines Clusters. Lokale Benutzer- und Gruppenobjekte werden in der RDB gespeichert.

Gründe für die Erstellung lokaler ONTAP SMB Benutzer und lokaler Gruppen

Es gibt mehrere Gründe für die Erstellung lokaler Benutzer und lokaler Gruppen auf Ihrer Storage Virtual Machine (SVM). Beispielsweise ist der Zugriff auf einen SMB-Server über ein lokales Benutzerkonto möglich, wenn die Domänencontroller (DCs) nicht verfügbar sind, lokale Gruppen können zur Zuweisung von Berechtigungen genutzt werden, oder der SMB-Server befindet sich in einer Arbeitsgruppe.

Aus folgenden Gründen kann ein oder mehrere lokale Benutzerkonten erstellt werden:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänenbenutzer sind nicht verfügbar.

  In Arbeitsgruppenkonfigurationen sind lokale Benutzer erforderlich.

- Es soll möglich sein, sich beim SMB-Server zu authentifizieren und anzumelden, falls die Domänencontroller nicht verfügbar sind.

  Lokale Benutzer können sich beim SMB-Server mittels NTLM-Authentifizierung anmelden, wenn der Domänencontroller ausgefallen ist oder wenn Netzwerkprobleme verhindern, dass der SMB-Server den Domänencontroller kontaktiert.

- Es besteht der Wunsch, einem lokalen Benutzer die Berechtigungen für die *User Rights Management* -Verwaltung zuzuweisen.

  User Rights Management ist die Fähigkeit eines SMB-Serveradministrators, die Rechte von Benutzern und Gruppen auf der SVM zu steuern. Sie können einem Benutzer Berechtigungen zuweisen, indem Sie die Berechtigungen dem Benutzerkonto zuweisen oder den Benutzer einer lokalen Gruppe hinzufügen, die über diese Berechtigungen verfügt.

Aus folgenden Gründen kann eine oder mehrere lokale Gruppen erstellt werden:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänengruppen sind nicht verfügbar.

  Lokale Gruppen sind in Arbeitsgruppen-Konfigurationen nicht erforderlich, können aber für die Verwaltung der Zugriffsrechte lokaler Arbeitsgruppenbenutzer nützlich sein.

- Der Zugriff auf Datei- und Ordnerressourcen soll mithilfe lokaler Gruppen für die Freigabe- und Zugriffskontrolle auf Dateiebene gesteuert werden.
- Es besteht der Wunsch, lokale Gruppen mit individuell angepassten *User Rights Management* -Berechtigungen zu erstellen.

  Einige integrierte Benutzergruppen verfügen über vordefinierte Berechtigungen. Um eine benutzerdefinierte Gruppe von Berechtigungen zuzuweisen, kann eine lokale Gruppe erstellt und mit den erforderlichen Berechtigungen versehen werden. Lokale Benutzer, Domänenbenutzer und Domänengruppen können anschließend zu der lokalen Gruppe hinzugefügt werden.

Verwandte Informationen

- Informationen zur lokalen Benutzerauthentifizierung
- Liste der unterstützten Berechtigungen

Informationen zur lokalen ONTAP SMB-Benutzerauthentifizierung

Bevor ein lokaler Benutzer auf Daten auf einem CIFS-Server zugreifen kann, muss er eine authentifizierte Sitzung erstellen.

Da SMB sitzungsbasiert ist, kann die Identität des Benutzers nur einmalig beim ersten Sitzungsaufbau ermittelt werden. Der CIFS-Server verwendet NTLM-basierte Authentifizierung bei der Authentifizierung lokaler Benutzer. Sowohl NTLMv1 als auch NTLMv2 werden unterstützt.

ONTAP verwendet die lokale Authentifizierung in drei Anwendungsfällen. Jeder Anwendungsfall hängt davon ab, ob der Domänenteil des Benutzernamens (im Format DOMAIN\user) mit dem lokalen Domänennamen des CIFS-Servers (dem CIFS-Servernamen) übereinstimmt:

- Der Domänenteil stimmt überein

  Benutzer, die bei der Anforderung des Datenzugriffs lokale Benutzeranmeldeinformationen angeben, werden lokal auf dem CIFS-Server authentifiziert.

- Der Domänenteil stimmt nicht überein

  ONTAP versucht, die NTLM-Authentifizierung mit einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört, durchzuführen. Bei erfolgreicher Authentifizierung ist die Anmeldung abgeschlossen. Wenn die Authentifizierung nicht erfolgreich ist, hängt das weitere Vorgehen davon ab, warum die Authentifizierung nicht erfolgreich war.

  Existiert der Benutzer beispielsweise in Active Directory, das Passwort ist jedoch ungültig oder abgelaufen, versucht ONTAP nicht, das entsprechende lokale Benutzerkonto auf dem CIFS-Server zu verwenden. Stattdessen schlägt die Authentifizierung fehl. Es gibt weitere Fälle, in denen ONTAP das entsprechende lokale Konto auf dem CIFS-Server für die Authentifizierung verwendet, sofern es existiert, auch wenn die NetBIOS-Domänennamen nicht übereinstimmen. Existiert beispielsweise ein passendes Domänenkonto, ist dieses jedoch deaktiviert, verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server für die Authentifizierung.

- Der Domänenteil ist nicht angegeben

  ONTAP versucht zunächst die Authentifizierung als lokaler Benutzer. Schlägt die Authentifizierung als lokaler Benutzer fehl, authentifiziert ONTAP den Benutzer bei einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört.

Nach erfolgreicher lokaler oder Domänen-Benutzerauthentifizierung erstellt ONTAP ein vollständiges Benutzerzugriffstoken, das die lokale Gruppenzugehörigkeit und Berechtigungen berücksichtigt.

Weitere Informationen zur NTLM-Authentifizierung für lokale Benutzer sind in der Microsoft Windows-Dokumentation zu finden.

Verwandte Informationen

Lokale Benutzerauthentifizierung auf Servern aktivieren oder deaktivieren

Informationen zu ONTAP SMB-Benutzerzugriffstoken

Wenn ein Benutzer eine Freigabe zuordnet, wird eine authentifizierte SMB-Sitzung hergestellt und ein Benutzerzugriffstoken erstellt, das Informationen über den Benutzer, die Gruppenzugehörigkeit des Benutzers und seine kumulativen Berechtigungen sowie den zugeordneten UNIX-Benutzer enthält.

Sofern diese Funktion nicht deaktiviert ist, werden dem Benutzerzugriffstoken auch lokale Benutzer- und Gruppeninformationen hinzugefügt. Die Art, wie Zugriffstoken erstellt werden, hängt davon ab, ob die Anmeldung für einen lokalen Benutzer oder einen Active Directory-Domänenbenutzer erfolgt:

- Lokale Benutzeranmeldung

  Obwohl lokale Benutzer Mitglieder verschiedener lokaler Gruppen sein können, können lokale Gruppen nicht Mitglieder anderer lokaler Gruppen sein. Das Zugriffstoken eines lokalen Benutzers setzt sich aus der Vereinigung aller Berechtigungen zusammen, die den Gruppen zugewiesen sind, denen der jeweilige lokale Benutzer angehört.

- Domänenbenutzeranmeldung

  Wenn sich ein Domänenbenutzer anmeldet, erhält ONTAP ein Benutzerzugriffstoken, das die Benutzer-SID und die SIDs aller Domänengruppen enthält, denen der Benutzer angehört. ONTAP verwendet die Vereinigung des Domänenbenutzerzugriffstokens mit dem Zugriffstoken, das durch lokale Mitgliedschaften der Domänengruppen des Benutzers bereitgestellt wird (sofern vorhanden), sowie alle direkt dem Domänenbenutzer oder einer seiner Domänengruppenmitgliedschaften zugewiesenen Berechtigungen.

Sowohl für die lokale als auch für die Domänenbenutzeranmeldung wird die primäre Gruppen-RID für das Benutzerzugriffstoken festgelegt. Die Standard-RID ist `Domain Users` (RID 513). Die Standardeinstellung kann nicht geändert werden.

Der Namenszuordnungsprozess zwischen Windows und UNIX sowie zwischen UNIX und Windows folgt für lokale und Domänenkonten denselben Regeln.

> Es gibt keine implizite, automatische Zuordnung eines UNIX-Benutzers zu einem lokalen Konto. Wenn dies erforderlich ist, muss eine explizite Zuordnungsregel mit den vorhandenen Namenszuordnungsbefehlen angegeben werden.

Die Auswirkungen der Löschung von ONTAP SMB-Servern auf Benutzer und Gruppen

Die Standardmenge an lokalen Benutzern und Gruppen wird bei der Erstellung eines CIFS-Servers angelegt und der Storage Virtual Machine (SVM) zugeordnet, die den CIFS-Server hostet. SVM-Administratoren können lokale Benutzer und Gruppen jederzeit erstellen. Es sollte beachtet werden, was mit den lokalen Benutzern und Gruppen geschieht, wenn der CIFS-Server gelöscht wird.

Lokale Benutzer und Gruppen sind SVMs zugeordnet, daher werden sie aus Sicherheitsgründen beim Löschen von CIFS-Servern nicht gelöscht. Obwohl lokale Benutzer und Gruppen beim Löschen des CIFS-Servers nicht gelöscht werden, sind sie ausgeblendet. Lokale Benutzer und Gruppen können erst wieder angezeigt oder verwaltet werden, nachdem ein CIFS-Server auf der SVM neu erstellt wurde.

> Der administrative Status des CIFS-Servers hat keinen Einfluss auf die Sichtbarkeit lokaler Benutzer oder Gruppen.

Die Verwendung der Microsoft Management Console mit lokalen ONTAP SMB-Benutzern und -Gruppen wird erläutert.

Informationen zu lokalen Benutzern und Gruppen können in der Microsoft Management Console angezeigt werden. Mit dieser Version von ONTAP ist es nicht möglich, andere Verwaltungsaufgaben für lokale Benutzer und Gruppen über die Microsoft Management Console durchzuführen.

Informationen zur Verwendung von SnapMirror auf ONTAP SMB SVMs, die lokale Gruppen enthalten

Es sind die Richtlinien zu beachten, wenn SnapMirror auf Volumes konfiguriert wird, die SVMs gehören und lokale Gruppen enthalten.

Lokale Gruppen können nicht in ACEs verwendet werden, die auf Dateien, Verzeichnisse oder Freigaben angewendet werden, die von SnapMirror auf eine andere SVM repliziert werden. Wenn die SnapMirror Funktion verwendet wird, um ein DR-Mirror für ein Volume auf einer anderen SVM zu erstellen und das Volume eine ACE für eine lokale Gruppe enthält, ist die ACE auf dem Mirror ungültig. Wenn Daten auf eine andere SVM repliziert werden, gelangen die Daten effektiv in eine andere lokale Domäne. Die Berechtigungen, die lokalen Benutzern und Gruppen gewährt werden, sind nur innerhalb des Gültigkeitsbereichs der SVM gültig, auf der sie ursprünglich erstellt wurden.

Erfahren Sie mehr über ONTAP SMB-Berechtigungen

Sie können Berechtigungen direkt lokalen Benutzern oder Domänenbenutzern zuweisen. Alternativ können Benutzer lokalen Gruppen zugeordnet werden, deren Berechtigungen den gewünschten Benutzerfunktionen entsprechen.

- Sie können einer von Ihnen erstellten Gruppe eine Reihe von Berechtigungen zuweisen.

  Anschließend wird ein Benutzer zu der Gruppe hinzugefügt, die über die Berechtigungen verfügt, die dieser Benutzer erhalten soll.

- Sie können außerdem lokale Benutzer und Domänenbenutzer vordefinierten Gruppen zuordnen, deren Standardberechtigungen den Berechtigungen entsprechen, die Sie diesen Benutzern gewähren möchten.

Verwandte Informationen

- Berechtigungen für lokale oder Domänenbenutzer oder Gruppen hinzufügen, entfernen oder zurücksetzen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Liste der unterstützten ONTAP SMB Berechtigungen

ONTAP verfügt über einen vordefinierten Satz unterstützter Berechtigungen. Bestimmten vordefinierten lokalen Gruppen sind einige dieser Berechtigungen standardmäßig zugewiesen. Es besteht außerdem die Möglichkeit, Berechtigungen zu den vordefinierten Gruppen hinzuzufügen oder zu entfernen oder neue lokale Benutzer oder Gruppen zu erstellen und den von Ihnen erstellten Gruppen oder bestehenden Domänenbenutzern und -gruppen Berechtigungen zuzuweisen.

Die folgende Tabelle listet die unterstützten Berechtigungen auf der Storage Virtual Machine (SVM) auf und enthält eine Liste der BUILTIN-Gruppen mit zugewiesenen Berechtigungen:

Berechtigungsname	Standard-Sicherheitseinstellung	Beschreibung
`SeTcbPrivilege`	Keine	Als Teil des Betriebssystems
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Dateien und Verzeichnisse sichern und dabei alle ACLs überschreiben
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Dateien und Verzeichnisse wiederherstellen und dabei alle ACLs überschreiben. Eine gültige Benutzer- oder Gruppen-SID als Dateibesitzer festlegen
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Besitz von Dateien oder anderen Objekten übernehmen
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Auditierung verwalten Dies umfasst das Anzeigen, Sichern und Löschen des Sicherheitsprotokolls.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Umgehung der Traversierungsprüfung Benutzer mit dieser Berechtigung benötigen keine Traverse-(x)-Berechtigungen, um Ordner, Symlinks oder Junctions zu durchlaufen.

Verwandte Informationen

- Informationen zur Zuweisung von Berechtigungen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Informationen zu BUILTIN Gruppen und lokalen Administrator Konten auf ONTAP SMB Servern

Bestimmte Richtlinien sind zu beachten, wenn integrierte Gruppen und das lokale Administratorkonto verwendet werden. Beispielsweise kann das lokale Administratorkonto umbenannt, jedoch nicht gelöscht werden.

- Das Administratorkonto kann umbenannt, aber nicht gelöscht werden.
- Das Administratorkonto kann nicht aus der Gruppe BUILTIN\Administrators entfernt werden.
- BUILTIN-Gruppen können umbenannt, aber nicht gelöscht werden.

  Nach der Umbenennung der BUILTIN-Gruppe kann ein weiteres lokales Objekt mit dem bekannten Namen erstellt werden; dem Objekt wird jedoch eine neue RID zugewiesen.

- Es existiert kein lokales Gastkonto.

Verwandte Informationen

Vordefinierte BUILTIN Gruppen und Standardberechtigungen

Anforderungen an lokale ONTAP SMB-Benutzerpasswörter

Standardmäßig müssen Passwörter lokaler Benutzer die Komplexitätsanforderungen erfüllen. Die Anforderungen an die Passwortkomplexität ähneln den in der Microsoft Windows *Lokalen Sicherheitsrichtlinie* definierten Anforderungen.

Das Passwort muss folgende Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf nicht den Benutzernamen enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
  - Englische Großbuchstaben (A bis Z)
  - Englische Kleinbuchstaben (a bis z)
  - Ziffern im Dezimalsystem (0 bis 9)
  - Sonderzeichen:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Verwandte Informationen

- Passwortkomplexität für lokale Benutzer konfigurieren
- Informationen zu den Server-Sicherheitseinstellungen
- Passwörter lokaler Benutzerkonten ändern

Vordefinierte BUILTIN Gruppen und standardmäßige ONTAP SMB-Berechtigungen

Sie können einem lokalen Benutzer oder Domänenbenutzer die Mitgliedschaft in einer vordefinierten Gruppe von BUILTIN-Gruppen zuweisen, die von ONTAP bereitgestellt werden. Vordefinierte Gruppen haben vordefinierte Berechtigungen zugewiesen.

Die folgende Tabelle beschreibt die vordefinierten Gruppen:

Vordefinierte BUILTIN Gruppe	Standardberechtigungen
`BUILTIN\Administrators`RID 544 Wenn das lokale `Administrator` Konto mit einer RID von 500 erstmals erstellt wird, wird es automatisch Mitglied dieser Gruppe. Wenn die Storage Virtual Machine (SVM) einer Domäne beitritt, wird die `domain\Domain Admins` Gruppe zur Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird die `domain\Domain Admins` Gruppe aus der Gruppe entfernt.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`

Vordefinierte BUILTIN Gruppe	Standardberechtigungen
`BUILTIN\Power Users`RID 547 Diese Gruppe hat bei ihrer Erstellung keine Mitglieder. Mitglieder dieser Gruppe weisen die folgenden Merkmale auf: • Kann lokale Benutzer und Gruppen erstellen und verwalten. • Kann sich selbst oder andere Objekte nicht zur `BUILTIN\Administrators` Gruppe hinzufügen.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Diese Gruppe hat bei ihrer Erstellung keine Mitglieder. Mitglieder dieser Gruppe können die Lese- und Schreibberechtigungen für Dateien oder Ordner überschreiben, wenn sie mit Backup-Absicht geöffnet werden.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Diese Gruppe hat nach ihrer Erstellung keine Mitglieder (abgesehen von der impliziten `Authenticated Users` Sondergruppe). Wenn die SVM einer Domäne beitritt, wird die `domain\Domain Users` Gruppe zu dieser Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird die `domain\Domain Users` Gruppe aus dieser Gruppe entfernt.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Diese Gruppe umfasst alle Benutzer, einschließlich Gäste (jedoch keine anonymen Benutzer). Es handelt sich um eine implizite Gruppe mit impliziter Mitgliedschaft.	`SeChangeNotifyPrivilege`

Verwandte Informationen

- Informationen zu BUILTIN Gruppen und lokalen Administrator Konten auf Servern
- Liste der unterstützten Berechtigungen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Aktivieren oder Deaktivieren der lokalen ONTAP SMB-Benutzer- und Gruppenfunktionalität

Bevor Sie lokale Benutzer und Gruppen für die Zugriffskontrolle von NTFS-Sicherheitsstil-Daten verwenden können, muss die Funktionalität für lokale Benutzer und Gruppen aktiviert sein. Zusätzlich muss die Funktionalität für die lokale Benutzerauthentifizierung aktiviert sein, wenn lokale Benutzer für die SMB-Authentifizierung verwendet werden sollen.

Die Funktionen für lokale Benutzer und Gruppen sowie die lokale Benutzerauthentifizierung sind

standardmäßig aktiviert. Falls sie nicht aktiviert sind, müssen sie aktiviert werden, bevor lokale Benutzer und Gruppen konfiguriert und verwendet werden können. Die Funktionen für lokale Benutzer und Gruppen können jederzeit deaktiviert werden.

Zusätzlich zur expliziten Deaktivierung der lokalen Benutzer- und Gruppenfunktionalität deaktiviert ONTAP die lokale Benutzer- und Gruppenfunktionalität auch, wenn ein Knoten im Cluster auf eine ONTAP Version zurückgesetzt wird, die diese Funktionalität nicht unterstützt. Die lokale Benutzer- und Gruppenfunktionalität ist erst aktiviert, wenn auf allen Knoten im Cluster eine Version von ONTAP ausgeführt wird, die sie unterstützt.

Verwandte Informationen

- Lokale Benutzerkonten ändern
- Lokale Gruppen ändern
- Berechtigungen für lokale oder Domänenbenutzer oder -gruppen hinzufügen

Lokale Benutzer und Gruppen auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können lokale Benutzer und Gruppen für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Funktionalität für lokale Benutzer und Gruppen ist standardmäßig aktiviert.

Über diese Aufgabe

Sie können lokale Benutzer und Gruppen bei der Konfiguration von SMB-Freigaben und NTFS-Dateiberechtigungen verwenden und optional lokale Benutzer für die Authentifizierung beim Erstellen einer SMB-Verbindung nutzen. Um lokale Benutzer für die Authentifizierung zu verwenden, muss außerdem die Option zur Authentifizierung lokaler Benutzer und Gruppen aktiviert werden.

Schritte

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

```
set -privilege advanced
```

2. Lokale Benutzer und Gruppen aktivieren oder deaktivieren:
   - Lokale Benutzer und Gruppen aktivieren:

```
vserver cifs options modify -vserver <SVM_name> -is-local-users-and
-groups-enabled true
```

   - Lokale Benutzer und Gruppen deaktivieren:

```
vserver cifs options modify -vserver <SVM_name> -is-local-users-and
-groups-enabled false
```

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel aktiviert die Funktionalität für lokale Benutzer und Gruppen auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

- Lokale Benutzerkonten verwalten == Lokale Benutzerauthentifizierung auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können die lokale Benutzerauthentifizierung für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Standardmäßig ist die lokale Benutzerauthentifizierung erlaubt, was nützlich ist, wenn die SVM keinen Domänencontroller erreichen kann oder wenn keine Zugriffskontrollen auf Domänenebene verwendet werden.

Bevor Sie beginnen

Die Funktionalität für lokale Benutzer und Gruppen muss auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie können die lokale Benutzerauthentifizierung jederzeit aktivieren oder deaktivieren. Wenn Sie lokale Benutzer für die Authentifizierung beim Erstellen einer SMB-Verbindung verwenden möchten, muss außerdem die Option „Lokale Benutzer und Gruppen“ des CIFS-Servers aktiviert werden.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Lokale Benutzerauthentifizierung aktivieren oder deaktivieren:
   - Lokale Benutzerauthentifizierung aktivieren:

     ```
     vserver cifs options modify -vserver <SVM_name> -is-local-auth
     -enabled true
     ```

   - Lokale Benutzerauthentifizierung deaktivieren:

     ```
     vserver cifs options modify -vserver <SVM_name> -is-local-auth
     ```

```
-enabled false
```

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel aktiviert die lokale Benutzerauthentifizierung auf SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

- Informationen zur lokalen Benutzerauthentifizierung
- Lokale Benutzer und Gruppen auf Servern aktivieren oder deaktivieren

Lokale ONTAP SMB-Benutzerkonten verwalten

Sie können ein lokales Benutzerkonto aktivieren, um den Zugriff auf SVM-Daten über SMB zu ermöglichen, oder das Konto deaktivieren, um den Zugriff zu verhindern. Sie können das Konto auch bearbeiten, um den vollständigen Namen, die Beschreibung oder den Aktivierungsstatus des Benutzers zu aktualisieren. Bei Bedarf können Sie das Konto aus administrativen Gründen umbenennen, beispielsweise bei einem kompromittierten Benutzernamen. Sie können außerdem die lokalen Gruppen anzeigen, denen ein Benutzer angehört, was hilft, den Datei- und Ordnerzugriff zu ermitteln und Zugriffsprobleme zu beheben.

Wenn Sie möchten…	Geben Sie den Befehl ein…
Ändern Sie das Passwort des lokalen Benutzers	`vserver cifs users-and-groups local-user set-password -vserver <SVM_name> -user-name <user_name>`
Lokales Benutzerkonto aktivieren oder deaktivieren	`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user-name <user_name> -is -account-disabled {true
false}`	Detaillierte Kontoinformationen für einen Benutzer anzeigen

Wenn Sie möchten…	Geben Sie den Befehl ein…
`vserver cifs users-and-groups local-user show -instance -vserver <SVM_name> -user-name <user_name>`	Informationen zur lokalen Benutzermitgliedschaft für einen bestimmten lokalen Benutzer anzeigen
`vserver cifs users-and-groups local-user show-membership -user-name <user_name>`	Anzeige der Mitgliedschaftsinformationen des lokalen Benutzers für die lokale Gruppe, der dieser lokale Benutzer angehört
`vserver cifs users-and-groups local-user show-membership -membership` *group_name*	Benutzermitgliedschaftsinformationen für lokale Benutzer, die einer bestimmten Storage Virtual Machine (SVM) zugeordnet sind, anzeigen
`vserver cifs users-and-groups local-user show-membership -vserver <SVM_name>`	Detaillierte Informationen zu allen lokalen Benutzern auf einer bestimmten SVM
`vserver cifs users-and-groups local-user show-membership -instance -vserver <SVM_name>`	Informationen zu allen Benutzern auf der Storage Virtual Machine (SVM) anzeigen
`vserver cifs users-and-groups local-user show -vserver <SVM_name>`	Die Beschreibung des lokalen Benutzers ändern
`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user -name <user_name> -description text` Enthält die Beschreibung ein Leerzeichen, so muss sie in doppelte Anführungszeichen gesetzt werden.	Den vollständigen Namen des lokalen Benutzers anpassen
`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user -name <user_name> -full-name text` Enthält der vollständige Name ein Leerzeichen, so muss er in doppelte Anführungszeichen gesetzt werden.	Das lokale Benutzerkonto umbenennen

Beispiel

Im folgenden Beispiel wird der lokale Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1 in “CIFS_SERVER\sue_new” umbenannt:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Beispiel

Das folgende Beispiel zeigt Informationen über alle lokalen Benutzer auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name     Description
-------- --------------------------- ------------- -------------
```

```
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Beispiel

Im folgenden Beispiel wird das Passwort für den lokalen Benutzer “CIFS_SERVER\sue” festgelegt, der der Storage Virtual Machine (SVM, früher bekannt als Vserver) vs1 zugeordnet ist:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Beispiel

Das folgende Beispiel zeigt die Mitgliedschaftsinformationen für alle lokalen Benutzer auf SVM vs1; Benutzer “CIFS_SERVER\Administrator” ist Mitglied der Gruppe “BUILTIN\Administrators”, und “CIFS_SERVER\sue” ist Mitglied der Gruppe “CIFS_SERVER\g1”:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                    Membership
---------- ---------------------------- ----------------------
vs1        CIFS_SERVER\Administrator    BUILTIN\Administrators
           CIFS_SERVER\sue              CIFS_SERVER\g1
```

Verwandte Informationen

- Weitere Informationen zu `vserver cifs` finden sich in der "ONTAP-Befehlsreferenz".
- Passwortkomplexität für lokale Benutzer konfigurieren
- Informationen zu den Server-Sicherheitseinstellungen

Lokale ONTAP SMB-Benutzerkonten löschen

Sie können lokale Benutzerkonten von Ihrer Storage Virtual Machine (SVM) löschen, wenn diese nicht mehr für die lokale SMB-Authentifizierung am CIFS-Server oder zur Ermittlung der Zugriffsrechte auf die auf Ihrer SVM enthaltenen Daten benötigt werden.

Über diese Aufgabe

Folgendes ist beim Löschen lokaler Benutzer zu beachten:

- Das Dateisystem bleibt unverändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die sich auf diesen Benutzer beziehen, werden nicht angepasst.

- Sämtliche Verweise auf lokale Benutzer werden aus den Mitgliedschafts- und Berechtigungsdatenbanken

entfernt.

- Standardmäßige, bekannte Benutzer wie Administrator können nicht gelöscht werden.

Schritte

1. Ermitteln Sie den Namen des lokalen Benutzerkontos, das Sie löschen möchten:

```
vserver cifs users-and-groups local-user show -vserver <SVM_name>
```

2. Löschen Sie den lokalen Benutzer:

```
vserver cifs users-and-groups local-user delete -vserver <SVM_name>
-user-name <user_name>
```

3. Überprüfen Sie, ob das Benutzerkonto gelöscht wurde:

```
vserver cifs users-and-groups local-user show -vserver <SVM_name>
```

Das folgende Beispiel löscht den lokalen Benutzer “CIFS_SERVER\sue”, der mit der SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Lokale ONTAP SMB-Gruppen verwalten

Sie können eine lokale Gruppe ändern, indem Sie ihre Beschreibung aktualisieren oder sie umbenennen. Sie können auch alle lokalen Gruppen im Cluster oder auf einer bestimmten Storage Virtual Machine (SVM) anzeigen und sehen, wer zu welcher Gruppe gehört. Diese Informationen können Ihnen bei der Fehlerbehebung von Dateizugriffs- und Benutzerrechtenproblemen auf der SVM helfen.

Wenn Sie möchten…	Verwenden Sie den Befehl…
Alle lokalen Gruppen im Cluster anzeigen	`vserver cifs users-and-groups local-group show`
Alle lokalen Gruppen auf der SVM anzeigen	`vserver cifs users-and-groups local-group show -vserver <SVM_name>`
Mitglieder aller lokalen Gruppen im Cluster anzeigen	`vserver cifs users-and-groups local-group show-members`
Mitglieder aller lokalen Gruppen auf der SVM anzeigen	`vserver cifs users-and-groups local-group show-members -vserver <SVM_name>`
Die Beschreibung der lokalen Gruppe ändern	`vserver cifs users-and-groups local-group modify -vserver <SVM_name> -group-name <group_name> -description text` Enthält die Beschreibung ein Leerzeichen, so muss sie in doppelte Anführungszeichen gesetzt werden.
Die lokale Gruppe umbenennen	`vserver cifs users-and-groups local-group rename -vserver <SVM_name> -group-name <group_name> -new -group-name <new_group_name>`

▼ **Befehlsbeispiele**

Beispiele

Im folgenden Beispiel wird die lokale Gruppe “CIFS_SERVER\engineering” in “CIFS_SERVER\engineering_new” umbenannt:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver
vs1 -group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

Das folgende Beispiel ändert die Beschreibung der lokalen Gruppe “CIFS_SERVER\engineering”:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver
vs1 -group-name CIFS_SERVER\engineering -description "New Description"
```

Beispiel

Das folgende Beispiel zeigt Informationen über alle lokalen Gruppen auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative
privileges
```

```
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Beispiel

Das folgende Beispiel zeigt Informationen über Mitglieder aller lokalen Gruppen auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ----------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Lokale ONTAP SMB-Gruppen löschen

Eine lokale Gruppe kann aus der Storage Virtual Machine (SVM) gelöscht werden, wenn sie nicht mehr für die Bestimmung der Zugriffsrechte auf Daten, die dieser SVM zugeordnet sind, benötigt wird oder wenn sie nicht mehr für die Zuweisung von SVM Benutzerrechten (Berechtigungen) an Gruppenmitglieder erforderlich ist.

Über diese Aufgabe

Folgendes ist beim Löschen lokaler Gruppen zu beachten:

- Das Dateisystem bleibt unverändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die auf diese Gruppe verweisen, sind nicht angepasst.

- Existiert die Gruppe nicht, wird ein Fehler zurückgegeben.
- Die spezielle Gruppe *Everyone* kann nicht gelöscht werden.
- Vordefinierte Gruppen wie *BUILTIN\Administrators BUILTIN\Users* können nicht gelöscht werden.

Schritte

1. Ermitteln Sie den Namen der lokalen Gruppe, die Sie löschen möchten, indem Sie die Liste der lokalen Gruppen auf dem SVM anzeigen:

   ```
   vserver cifs users-and-groups local-group show -vserver <SVM_name>
   ```

2. Lokale Gruppe löschen:

   ```
   vserver cifs users-and-groups local-group delete -vserver <SVM_name>
   ```

```
-group-name <group_name>
```

3. Überprüfen Sie, ob die Gruppe gelöscht wurde:

```
vserver cifs users-and-groups local-group show -vserver <SVM_name>
```

▼ **Befehlsbeispiel**

Das folgende Beispiel löscht die lokale Gruppe “CIFS_SERVER\sales”, die mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- ----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver
vs1 -group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- ----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

Fügen Sie ein Mitglied zu einer lokalen ONTAP SMB-Gruppe hinzu

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale Benutzer, Domänenbenutzer oder Domänengruppen hinzufügen. Dies ist hilfreich, wenn Sie den Zugriff auf Daten basierend auf den für die Gruppe festgelegten Zugriffskontrollen steuern oder wenn Sie möchten, dass Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten.

Über diese Aufgabe

- Sie können keine Benutzer zur speziellen Gruppe *Everyone* hinzufügen.
- Die lokale Gruppe muss existieren, bevor Sie einen Benutzer hinzufügen können.
- Der Benutzer muss existieren, bevor Sie ihn einer lokalen Gruppe hinzufügen können.

- Sie können keine lokale Gruppe zu einer anderen lokalen Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Domänengruppe zu einer lokalen Gruppe hinzuzufügen, muss Data ONTAP den Namen in eine SID auflösen können.

Schritt

1. Füge ein Mitglied zu einer Gruppe hinzu:

```
vserver cifs users-and-groups local-group add-members -vserver
_vserver_name_ -group-name _group_name_ -member-names name[,...]
```

Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die zur angegebenen lokalen Gruppe hinzugefügt werden.

▼ Befehlsbeispiel

Das folgende Beispiel fügt den lokalen Benutzer “SMB_SERVER\sue” und die Domänengruppe “AD_DOM\dom_eng” der lokalen Gruppe “SMB_SERVER\engineering” auf SVM vs1 hinzu:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

Ein Mitglied aus einer lokalen ONTAP SMB-Gruppe entfernen

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale Benutzer, Domänenbenutzer oder Domänengruppen entfernen. Dies ist hilfreich, wenn Sie den Zugriff auf Daten basierend auf den für die Gruppe festgelegten Zugriffskontrollen steuern oder wenn Sie möchten, dass Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten.

Über diese Aufgabe

- Sie können keine Mitglieder aus der speziellen Gruppe *Everyone* entfernen.
- Die Gruppe, aus der Sie ein Mitglied entfernen möchten, muss existieren.
- ONTAP muss in der Lage sein, die Namen der Mitglieder, die aus der Gruppe entfernt werden sollen, in eine entsprechende SID aufzulösen.

Schritt

1. Ein Mitglied aus einer Gruppe entfernen:

```
vserver cifs users-and-groups local-group remove-members -vserver
_vserver_name_ -group-name _group_name_ -member-names name[,...]
```

Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden.

▼ Befehlsbeispiel

Das folgende Beispiel entfernt die lokalen Benutzer “SMB_SERVER\sue” und “SMB_SERVER\james” aus der lokalen Gruppe “SMB_SERVER\engineering” auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

ONTAP SMB-Domänenbenutzer- und Gruppennamen in lokalen Datenbanken aktualisieren

Sie können Domänenbenutzer und -gruppen zu den lokalen Gruppen eines CIFS-Servers hinzufügen. Diese Domänenobjekte werden in lokalen Datenbanken im Cluster registriert. Wenn ein Domänenobjekt umbenannt wird, müssen die lokalen Datenbanken manuell aktualisiert werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) angeben, auf der Sie die Domänennamen aktualisieren möchten.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Aktualisieren Sie die Namen der Domänenbenutzer und -gruppen, die der Storage Virtual Machine zugeordnet sind:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name>
   ```

3. Anzeige der Domänenbenutzer und -gruppen, deren Aktualisierung erfolgreich war und deren Aktualisierung fehlgeschlagen ist:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name> -display
   -failed-only false|true
   ```

4. Um alle Statusinformationen zu Aktualisierungen zu unterdrücken, verwenden Sie folgenden Befehl:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name> -suppress
   -all-output true
   ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

▼ Befehlsbeispiel

Das folgende Beispiel aktualisiert die Namen der Domänenbenutzer und -gruppen, die der Storage Virtual Machine (SVM, ehemals Vserver) vs1 zugeordnet sind. Für die letzte Aktualisierung besteht eine abhängige Namenskette, die aktualisiert werden muss:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Verwandte Informationen

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

Berechtigungen für ONTAP SMB lokale oder Domänenbenutzer oder -gruppen verwalten

Berechtigungen zu ONTAP SMB lokalen oder Domänenbenutzern oder -gruppen hinzufügen

Sie können die Benutzerrechte für lokale oder Domänenbenutzer oder -gruppen verwalten, indem Sie Berechtigungen hinzufügen. Die hinzugefügten Berechtigungen überschreiben die standardmäßig zugewiesenen Berechtigungen für eines dieser Objekte. Dies bietet eine verbesserte Sicherheit, da sich individuell festlegen lässt, über welche Berechtigungen ein Benutzer oder eine Gruppe verfügt.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer bzw. die Gruppe, zu der Berechtigungen hinzugefügt werden, muss bereits existieren.

Über diese Aufgabe

Das Hinzufügen einer Berechtigung zu einem Objekt überschreibt die Standardberechtigungen für diesen Benutzer oder diese Gruppe. Das Hinzufügen einer Berechtigung entfernt zuvor hinzugefügte Berechtigungen nicht.

Beim Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -gruppen ist Folgendes zu beachten:

- Sie können eine oder mehrere Berechtigungen hinzufügen.
- Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren.

  Der Befehl kann fehlschlagen, wenn ONTAP keinen Kontakt zum Domänencontroller herstellen kann.

Schritte

1. Fügen Sie einem lokalen Benutzer, einem Domänenbenutzer oder einer Gruppe eine oder mehrere Berechtigungen hinzu:

```
vserver cifs users-and-groups privilege add-privilege -vserver
<SVM_name> -user-or-group-name <name> -privileges <privilege>[,...]
```

2. Überprüfen Sie, ob dem Objekt die gewünschten Berechtigungen zugewiesen wurden:

```
vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
-or-group-name <name>
```

Beispiel

Das folgende Beispiel fügt die Berechtigungen “SeTcbPrivilege” und “SeTakeOwnershipPrivilege” dem Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1 hinzu:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Berechtigungen von ONTAP SMB lokalen oder Domänenbenutzern oder -gruppen entfernen

Sie können die Benutzerrechte für lokale oder Domänenbenutzer oder -gruppen verwalten, indem Sie Berechtigungen entfernen. Dies bietet eine höhere Sicherheit, da Sie die maximalen Berechtigungen von Benutzern und Gruppen individuell anpassen können.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer oder die Gruppe, von der Berechtigungen entfernt werden, muss bereits existieren.

Über diese Aufgabe

Beim Entfernen von Berechtigungen für lokale oder Domänenbenutzer oder -gruppen ist Folgendes zu beachten:

- Sie können eine oder mehrere Berechtigungen entfernen.
- Beim Entfernen von Berechtigungen von einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren.

  Der Befehl kann fehlschlagen, wenn ONTAP keinen Kontakt zum Domänencontroller herstellen kann.

Schritte

1. Einem lokalen Benutzer, einem Domänenbenutzer oder einer Gruppe eine oder mehrere Berechtigungen entziehen:

   ```
   vserver cifs users-and-groups privilege remove-privilege -vserver
   <SVM_name> -user-or-group-name <name> -privileges <privilege>[,...]
   ```

2. Überprüfen Sie, ob die gewünschten Berechtigungen vom Objekt entfernt wurden:

   ```
   vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
   -or-group-name <name>
   ```

Beispiel

Das folgende Beispiel entfernt die Berechtigungen “SeTcbPrivilege” und “SeTakeOwnershipPrivilege” vom Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
```

```
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------
vs1       CIFS_SERVER\sue       -
```

Berechtigungen für ONTAP SMB lokale oder Domänenbenutzer und -gruppen zurücksetzen

Sie können die Berechtigungen für lokale oder Domänenbenutzer und -gruppen zurücksetzen. Dies kann hilfreich sein, wenn Berechtigungen für einen lokalen oder Domänenbenutzer oder eine Gruppe geändert wurden und diese Änderungen nicht mehr gewünscht oder benötigt werden.

Über diese Aufgabe

Das Zurücksetzen der Berechtigungen für einen lokalen oder Domänenbenutzer oder eine lokale oder Domänengruppe entfernt sämtliche Berechtigungseinträge für dieses Objekt.

Schritte

1. Setzen Sie die Berechtigungen für einen lokalen oder Domänenbenutzer oder eine lokale oder Domänengruppe zurück:

   ```
   vserver cifs users-and-groups privilege reset-privilege -vserver
   <SVM_name> -user-or-group-name <name>
   ```

2. Überprüfen Sie, ob die Berechtigungen für das Objekt zurückgesetzt wurden:

   ```
   vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
   -or-group-name <name>
   ```

Beispiele

Das folgende Beispiel setzt die Berechtigungen des Benutzers “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1 zurück. Standardmäßig sind normalen Benutzern keine Berechtigungen zugeordnet:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Das folgende Beispiel setzt die Berechtigungen für die Gruppe “BUILTIN\Administrators” zurück, wodurch der Berechtigungseintrag entfernt wird:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Informationen zu ONTAP SMB-Berechtigungsüberschreibungen

Sie können Informationen über benutzerdefinierte Berechtigungen anzeigen, die Domänen- oder lokalen Benutzerkonten oder Gruppen zugewiesen sind. Diese Informationen helfen Ihnen festzustellen, ob die gewünschten Benutzerrechte angewendet werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie diesen Befehl ein…
Benutzerdefinierte Berechtigungen für alle Domänen- und lokalen Benutzer und Gruppen auf der Storage Virtual Machine (SVM)	`vserver cifs users-and-groups privilege show -vserver <SVM_name>`
Benutzerdefinierte Berechtigungen für eine bestimmte Domäne oder einen lokalen Benutzer und eine Gruppe auf der SVM	`vserver cifs users-and-groups privilege show -vserver <SVM_name> -user-or-group-name <name>`

   Es gibt weitere optionale Parameter, die Sie beim Ausführen dieses Befehls auswählen können. Weitere Informationen zu `vserver cifs users-and-groups privilege show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Der folgende Befehl zeigt alle Berechtigungen an, die lokalen oder Domänenbenutzern und -gruppen für SVM

vs1 explizit zugeordnet sind:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- --------------------   ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Umgehungsüberprüfung konfigurieren

Informationen zur Konfiguration der ONTAP SMB Bypass Traverse-Prüfung

Die Umgehung der Pfadprüfung ist ein Benutzerrecht (auch als Berechtigung bezeichnet), das festlegt, ob ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, selbst wenn er keine Berechtigung für das durchlaufene Verzeichnis besitzt. Es ist wichtig zu verstehen, was geschieht, wenn die Umgehung der Pfadprüfung erlaubt oder nicht erlaubt wird, und wie die Umgehung der Pfadprüfung für Benutzer auf Storage Virtual Machines (SVMs) konfiguriert werden kann.

Was geschieht beim Zulassen oder Verweigern der Bypass Traverse-Prüfung

- Sofern zulässig, prüft ONTAP beim Versuch eines Benutzers, auf eine Datei zuzugreifen, nicht die Traverse-Berechtigung für die Zwischenverzeichnisse, wenn entschieden wird, ob der Zugriff auf die Datei gewährt oder verweigert wird.
- Falls dies nicht zulässig ist, prüft ONTAP die Ausführungsberechtigung für alle Verzeichnisse im Pfad zur Datei.

  Wenn eines der Zwischenverzeichnisse nicht über die Berechtigung “X” (Durchlaufberechtigung) verfügt, verweigert ONTAP den Zugriff auf die Datei.

Umgehungsüberprüfung konfigurieren

Die Umgehung der Traverse-Prüfung kann mithilfe der ONTAP CLI oder durch die Konfiguration von Active Directory Gruppenrichtlinien mit diesem Benutzerrecht eingerichtet werden.

Die `SeChangeNotifyPrivilege`Berechtigung steuert, ob Benutzern das Umgehen der Traverse-Prüfung erlaubt ist.

- Das Hinzufügen zu lokalen SMB-Benutzern oder -Gruppen auf der SVM oder zu Domänenbenutzern oder -gruppen ermöglicht das Umgehen der Traverse-Prüfung.
- Das Entfernen aus den lokalen SMB-Benutzern oder Gruppen auf der SVM oder aus den Domänenbenutzern oder Gruppen verhindert die Umgehung der Traverse-Prüfung.

Standardmäßig haben die folgenden BUILTIN-Gruppen auf dem SVM das Recht, die Traversierungsprüfung zu umgehen:

- `BUILTIN\Administrators`

- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Wenn nicht gewünscht ist, dass Mitglieder einer dieser Gruppen die Traverse-Prüfung umgehen, muss dieser Gruppe diese Berechtigung entzogen werden.

Bei der Konfiguration der Umgehung der Traverse-Prüfung für lokale SMB-Benutzer und -Gruppen auf der SVM mithilfe der CLI ist Folgendes zu beachten:

- Wenn Mitglieder einer benutzerdefinierten lokalen oder Domänengruppe die Traverse-Prüfung umgehen dürfen, muss der Gruppe die `SeChangeNotifyPrivilege` Berechtigung hinzugefügt werden.
- Wenn einem einzelnen lokalen Benutzer oder Domänenbenutzer erlaubt werden soll, die Überprüfung der Zugriffsrechte zu umgehen, und dieser Benutzer kein Mitglied einer Gruppe mit dieser Berechtigung ist, kann die `SeChangeNotifyPrivilege` Berechtigung diesem Benutzerkonto hinzugefügt werden.
- Sie können die Umgehung der Traverse-Prüfung für lokale oder Domänenbenutzer oder -gruppen deaktivieren, indem Sie die `SeChangeNotifyPrivilege`Berechtigung jederzeit entfernen.

> Um die Überprüfung von Bypass-Travers für bestimmte lokale oder Domänenbenutzer oder -gruppen zu deaktivieren, muss außerdem die `SeChangeNotifyPrivilege` Berechtigung aus der `Everyone` Gruppe entfernt werden.

Verwandte Informationen

- Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung erlauben
- Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung untersagen
- Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren
- Freigabe-Zugriffskontrolllisten erstellen
- Sicherer Dateizugriff mit Storage Level Access Guard
- Liste der unterstützten Berechtigungen
- Berechtigungen für lokale oder Domänenbenutzer oder -gruppen hinzufügen

Benutzern oder Gruppen erlauben, die ONTAP SMB-Verzeichnisdurchlaufprüfung zu umgehen

Wenn ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen können soll, auch wenn er für ein durchlaufenes Verzeichnis keine Berechtigungen hat, kann die `SeChangeNotifyPrivilege` Berechtigung lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) hinzugefügt werden. Standardmäßig können Benutzer die Überprüfung des Verzeichnisdurchlaufs umgehen.

Bevor Sie beginnen

- Auf der SVM muss ein SMB Server vorhanden sein.
- Die Option „Lokale Benutzer und Gruppen SMB-Server“ muss aktiviert sein.
- Der lokale oder Domänenbenutzer bzw. die Gruppe, zu der die `SeChangeNotifyPrivilege`Berechtigung hinzugefügt wird, muss bereits existieren.

Über diese Aufgabe

Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren. Der Befehl kann fehlschlagen, wenn ONTAP den Domänencontroller nicht erreichen kann.

Schritte

1. Die Umgehung der Traverse-Prüfung kann aktiviert werden, indem die `SeChangeNotifyPrivilege` -Berechtigung einem lokalen oder Domänenbenutzer oder einer Gruppe hinzugefügt wird: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group -name` *`name`* `-privileges SeChangeNotifyPrivilege`

   Der Wert für den `-user-or-group-name` Parameter ist ein lokaler Benutzer oder eine lokale Gruppe oder ein Domänenbenutzer oder eine Domänengruppe.

2. Es sollte überprüft werden, ob für den angegebenen Benutzer oder die Gruppe die Umgehung der Traversierungsprüfung aktiviert ist: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Der folgende Befehl ermöglicht es Benutzern der Gruppe “EXAMPLE\eng”, die Verzeichnisdurchsuchungsprüfung zu umgehen, indem die `SeChangeNotifyPrivilege` Berechtigung der Gruppe hinzugefügt wird:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Verwandte Informationen

Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung untersagen

Benutzern oder Gruppen das Umgehen der ONTAP SMB-Verzeichnisdurchlaufprüfung untersagen

Wenn nicht gewünscht ist, dass ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchläuft, weil der Benutzer keine Berechtigungen für das durchlaufene Verzeichnis hat, kann die `SeChangeNotifyPrivilege` Berechtigung von lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) entfernt werden.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer oder die Gruppe, von der Berechtigungen entfernt werden, muss bereits existieren.

Über diese Aufgabe

Beim Entfernen von Berechtigungen von einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren. Der Befehl kann fehlschlagen, wenn ONTAP den Domänencontroller nicht erreichen kann.

Schritte

1. Umgehung der Traversierungsprüfung nicht zulassen: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   Der Befehl entfernt die `SeChangeNotifyPrivilege`Berechtigung vom lokalen oder Domänen-Benutzer oder der Gruppe, die mit dem Wert für den `-user-or-group-name *name*`Parameter angegeben wird.

2. Es sollte überprüft werden, ob für den angegebenen Benutzer oder die Gruppe die Umgehung der Traversierungsprüfung deaktiviert ist: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Beispiel

Der folgende Befehl verhindert, dass Benutzer der Gruppe “EXAMPLE\eng” die Verzeichnisdurchsuchungsprüfung umgehen:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          -
```

Verwandte Informationen

Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung erlauben

Informationen zu Dateisicherheit und Überwachungsrichtlinien

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

Informationen zur Dateisicherheit von Dateien und Verzeichnissen in Volumes auf Storage Virtual Machines (SVMs) können angezeigt werden. Informationen zu Überwachungsrichtlinien auf FlexVol volumes können angezeigt werden. Wenn konfiguriert, können Informationen zu Storage-Level Access Guard und Dynamic Access Control Sicherheitseinstellungen auf FlexVol volumes angezeigt werden.

Anzeige von Informationen zur Dateisicherheit

Es lassen sich Informationen über die auf Daten in Volumes und Qtrees (für FlexVol volumes) angewendete Dateisicherheit mit den folgenden Sicherheitsstilen anzeigen:

- NTFS
- UNIX
- Gemischt

Anzeige von Informationen über Prüfungsrichtlinien

Informationen zu Überwachungsrichtlinien für die Überwachung von Zugriffsereignissen auf FlexVol volumes über die folgenden NAS-Protokolle können angezeigt werden:

- SMB (alle Versionen)
- NFSv4.x

Anzeige von Informationen zur Storage-Level Access Guard (SLAG) Sicherheit

Die Storage-Level Access Guard-Sicherheit kann auf FlexVol volumes und qtree-Objekte mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt
- UNIX (wenn auf der SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist)

Anzeigen von Informationen zur Dynamic Access Control (DAC) Sicherheit

Die Dynamic Access Control-Sicherheit kann auf ein Objekt innerhalb eines FlexVol volume mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt (wenn das Objekt über effektive NTFS-Sicherheit verfügt)

Verwandte Informationen

- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard
- Informationen zu Storage-Level Access Guard auf Servern

Informationen zur ONTAP SMB-Dateisicherheit auf NTFS Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf NTFS-Sicherheitsstil-Volumes anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu DOS-Attributen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- Da NTFS Security-Style Volumes und Qtrees ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte verwenden, enthalten UNIX-bezogene Ausgabefelder lediglich zur Anzeige bestimmte UNIX-Dateiberechtigungsinformationen.

- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Storage-Level Access Guard Sicherheit auf dem Volume-Root oder Qtree konfiguriert werden kann, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei-ACLs als auch Storage-Level Access Guard ACLs anzeigen.
- Die Ausgabe zeigt außerdem Informationen über die ACEs der Dynamic Access Control an, falls Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/vol4` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Das folgende Beispiel zeigt die Sicherheitsinformationen mit erweiterten Masken zum Pfad `/data/engineering` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
```

```
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
```

```
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...0 .... .... .... .... .... =
Synchronize
                            .... .... .... 0... .... .... .... .... =
Write Owner
                            .... .... .... .0.. .... .... .... .... =
Write DAC
                            .... .... .... ..0. .... .... .... .... =
Read Control
                            .... .... .... ...0 .... .... .... .... =
Delete
                            .... .... .... .... .... ...0 .... .... =
Write Attributes
                            .... .... .... .... .... .... 0... .... =
Read Attributes
                            .... .... .... .... .... .... .0.. .... =
Delete Child
                            .... .... .... .... .... .... ..0. .... =
Execute
                            .... .... .... .... .... .... ...0 .... =
Write EA
                            .... .... .... .... .... .... .... 0... =
Read EA
                            .... .... .... .... .... .... .... .0.. =
Append
                            .... .... .... .... .... .... .... ..0. =
Write
                            .... .... .... .... .... .... .... ...0 =
Read
```

Das folgende Beispiel zeigt Sicherheitsinformationen, einschließlich Storage-Level Access Guard-Sicherheitsinformationen, für das Volume mit dem Pfad `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

               Vserver: vs1
             File Path: /datavol1
     File Inode Number: 77
        Security Style: ntfs
       Effective Style: ntfs
        DOS Attributes: 10
 DOS Attributes in Text: ----D---
```

```
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form

oder als detaillierte Liste angezeigt werden.

- Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Ordner enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.
- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder effektive UNIX- oder NTFS-Sicherheit haben.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl UNIX-Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit effektiver NTFS-Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/projects` in SVM vs1 in erweiterter Maskenform. Dieser Pfad mit gemischtem Security-Style hat effektive UNIX-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
     File Inode Number: 78
        Security Style: mixed
       Effective Style: unix
        DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
```

```
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/data` in SVM vs1. Dieser Pfad mit gemischtem Sicherheitsstil hat eine effektive NTFS-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
                Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                 Unix Mode Bits in Text: rwxrwxrwx
                                   ACLs: NTFS Security Descriptor
                                         Control:0x8004
                                         Owner:BUILTIN\Administrators
                                         Group:BUILTIN\Administrators
                                         DACL - ACEs
                                           ALLOW-Everyone-0x1f01ff
                                           ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Volume am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Mixed Security-Style Volumes verfügt über effektive UNIX-Sicherheit. Das Volume verfügt über Storage-Level Access Guard-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
```

```
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf NTFS Security-Style-Volumes
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf UNIX Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf UNIX Security-Style-Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und -Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Verzeichnissicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- UNIX Security-Style-Volumes und Qtrees verwenden zur Bestimmung der Dateizugriffsrechte ausschließlich UNIX-Dateiberechtigungen, entweder Modusbits oder NFSv4-ACLs.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Eigentümer“ und „Gruppe“ in der ACL-Ausgabe gelten nicht für NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren aussagekräftig.

- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/home` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
```

```
                    Unix Mode Bits in Text: rwx------
                                      ACLs: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/home` in SVM vs1 in erweiterter Maskenform:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                        Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                  ACLs: -
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf Security-Style-Volumes anzeigen
- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

ONTAP Befehle zur Anzeige von Informationen über NTFS-Überwachungsrichtlinien auf SMB FlexVol Volumes

Sie können Informationen zu NTFS-Überwachungsrichtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- NTFS Security-Style Volumes und Qtrees verwenden ausschließlich NTFS-Systemzugriffskontrolllisten (SACLs) für Audit-Richtlinien.
- Auf Dateien und Ordner in einem Volume mit gemischtem Sicherheitsstil und effektiver NTFS-Sicherheit können NTFS-Überwachungsrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NTFS-SACLs enthalten oder auch nicht.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei- und Ordner-NFSv4-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS effektiver Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Bei der Anzeige von Sicherheitsinformationen zu Dateien und Ordnern mit NTFS effektiver Sicherheit enthalten die UNIX-bezogenen Ausgabefelder nur Anzeigeinformationen zu UNIX-Dateiberechtigungen.

  Dateien und Ordner im NTFS-Sicherheitsstil verwenden ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte.

- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige der Überwachungsrichtlinieneinstellungen für Dateien und Verzeichnisse mit dem gewünschten Detaillierungsgrad:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Als detaillierte Liste	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/corp` in SVM vs1. Der Pfad verfügt über effektive NTFS-Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen SUCCESS-

als auch einen SUCCESS/FAIL-SACL-Eintrag.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/datavol1` in SVM vs1. Der Pfad enthält sowohl reguläre Datei- und Ordner-SACLs als auch Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
```

```
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP Befehle zur Anzeige von Informationen zu NFSv4-Überwachungsrichtlinien auf SMB FlexVol volumes

Es lassen sich Informationen zu NFSv4-Auditrichtlinien auf FlexVol volumes mithilfe der ONTAP CLI anzeigen, darunter die Sicherheitsstile und effektiven Sicherheitsstile, die angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten (SACLs). Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Verzeichnissen angeben, deren Audit-Informationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- UNIX Security-Style Volumes und Qtrees verwenden ausschließlich NFSv4 SACLs für Audit-Richtlinien.
- Auf Dateien und Verzeichnisse in einem Volume mit gemischtem Sicherheitsstil, die dem UNIX-Sicherheitsstil entsprechen, können NFSv4-Auditrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten,

die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NFSv4-SACLs enthalten oder auch nicht.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritte

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/lab` in SVM vs1. Dieser UNIX-Sicherheitsstil-Pfad verfügt über eine NFSv4-SACL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
```

```
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

Sie können das Platzhalterzeichen (*) verwenden, um Informationen über die Dateisicherheit und die Revisionsprotokollrichtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Stammvolume anzuzeigen.

Das Platzhalterzeichen (**) kann als letzter Bestandteil eines angegebenen Verzeichnispfads verwendet werden, unterhalb dessen Informationen zu allen Dateien und Verzeichnissen angezeigt werden. Wenn Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „**“ angezeigt werden sollen, ist der vollständige Pfad in doppelte Anführungszeichen („``“) anzugeben.

Beispiel

Der folgende Befehl mit dem Platzhalterzeichen zeigt die Informationen zu allen Dateien und Verzeichnissen unterhalb des Pfads `/1/` von SVM vs1 an:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
          Security Style: mixed
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 0
           Unix Group Id: 0
          Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                    ACLs: NTFS Security Descriptor
                          Control:0x8514
                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                          ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
```

```
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Der folgende Befehl zeigt die Informationen einer Datei mit dem Namen "*" unter dem Pfad `/vol1/a` von SVM vs1 an. Der Pfad ist in doppelte Anführungszeichen (" ") eingeschlossen.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf SVMs mithilfe der CLI verwalten

ONTAP Befehle zur Verwaltung der SMB NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und des Storage-Level Access Guard

Die NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf Storage Virtual Machines (SVMs) lassen sich mithilfe der CLI verwalten.

Die NTFS-Dateisicherheit und Überwachungsrichtlinien können von SMB-Clients oder über die CLI verwaltet werden. Die Verwendung der CLI zur Konfiguration von Dateisicherheit und Überwachungsrichtlinien macht es jedoch unnötig, einen Remote-Client zur Verwaltung der Dateisicherheit zu nutzen. Die Nutzung der CLI kann die Zeit, die für das Anwenden von Sicherheitsmaßnahmen auf viele Dateien und Ordner mit einem einzigen Befehl benötigt wird, erheblich verkürzen.

Sie können Storage-Level Access Guard konfigurieren, eine zusätzliche Sicherheitsebene, die von ONTAP auf SVM-Volumes angewendet wird. Storage-Level Access Guard gilt für Zugriffe aller NAS-Protokolle auf das Speicherobjekt, auf das Storage-Level Access Guard angewendet wird.

Storage-Level Access Guard kann nur über die ONTAP-Befehlszeile konfiguriert und verwaltet werden. Einstellungen von Storage-Level Access Guard können nicht von SMB-Clients aus verwaltet werden. Zudem wird beim Anzeigen der Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client die Storage-Level Access Guard-Sicherheit nicht angezeigt. Die Storage-Level Access Guard-Sicherheit kann von einem Client, selbst durch einen Systemadministrator (Windows oder UNIX), nicht aufgehoben werden. Storage-Level Access Guard bietet daher eine zusätzliche Sicherheitsebene für den Datenzugriff, die unabhängig vom Speicheradministrator festgelegt und verwaltet wird.

> Auch wenn für Storage-Level Access Guard nur NTFS-Zugriffsberechtigungen unterstützt werden, kann ONTAP Sicherheitsprüfungen für den Zugriff über NFS auf Daten auf Volumes durchführen, auf denen Storage-Level Access Guard angewendet wird, wenn der UNIX-Benutzer einem Windows-Benutzer auf der SVM zugeordnet ist, der das Volume besitzt.

NTFS Security-Style Volumes

Alle Dateien und Ordner in NTFS Security-Style-Volumes und Qtrees verfügen über effektive NTFS-Sicherheit. Die `vserver security file-directory` Befehlsfamilie ermöglicht die Implementierung der folgenden Sicherheitsarten auf NTFS Security-Style-Volumes:

- Dateiberechtigungen und Überwachungsrichtlinien für Dateien und Ordner im Volume
- Storage-Level Access Guard-Sicherheit auf Volumes

Volumes mit gemischtem Security-Style

Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Ordner enthalten, die über UNIX-effektive Sicherheit verfügen und UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4.x-ACLs und NFSv4.x-Überwachungsrichtlinien, sowie einige Dateien und Ordner, die über NTFS-effektive Sicherheit verfügen und NTFS-Dateiberechtigungen und Überwachungsrichtlinien verwenden. Mit der `vserver security file-directory`Befehlsfamilie lassen sich die folgenden Sicherheitstypen auf Daten mit gemischtem Security-Style anwenden:

- Dateiberechtigungen und Überwachungsrichtlinien für Dateien und Ordner mit NTFS-Effektivsicherheitsstil im gemischten Volume oder qtree
- Storage-Level Access Guard für Volumes mit entweder NTFS- oder UNIX-effektivem Sicherheitsstil

UNIX Security-Style Volumes

UNIX Security-Style-Volumes und Qtrees enthalten Dateien und Ordner mit effektiver UNIX-Sicherheit (entweder Mode-Bits oder NFSv4.x-ACLs). Folgendes ist zu beachten, wenn die `vserver security file-directory` Command-Family zur Implementierung von Sicherheit auf UNIX Security-Style-Volumes verwendet wird:

- Die `vserver security file-directory`Befehlsfamilie kann nicht zur Verwaltung von UNIX-Dateisicherheits- und Überwachungsrichtlinien auf UNIX Security-Style Volumes und qtrees verwendet werden.
- Die `vserver security file-directory`Befehlsfamilie kann zur Konfiguration von Storage-Level Access Guard auf UNIX-Sicherheitsvolumes verwendet werden, sofern die SVM mit dem Ziel-Volume einen CIFS-Server enthält.

Verwandte Informationen

- Informationen zur Anzeige von Dateisicherheits- und Prüfrichtlinien
- NTFS-Sicherheitsdeskriptoren auf Servern erstellen
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner
- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard

ONTAP Befehle zum Festlegen der SMB-Datei- und Ordnersicherheit

Da Sie die Datei- und Ordnersicherheit lokal anwenden und verwalten können, ohne dass ein Remote-Client beteiligt ist, kann die Zeit für die Massensicherheitsfestlegung bei einer großen Anzahl von Dateien oder Ordnern erheblich reduziert werden.

Die Verwendung der Befehlszeilenschnittstelle (CLI) zum Festlegen der Datei- und Ordnersicherheit kann in folgenden Anwendungsfällen von Vorteil sein:

- Speicherung von Dateien in großen Unternehmensumgebungen, wie zum Beispiel Dateispeicherung in Home-Verzeichnissen
- Migration von Daten
- Änderung der Windows-Domäne
- Standardisierung von Dateisicherheits- und Überwachungsrichtlinien für NTFS-Dateisysteme

Informationen zu den Grenzen bei der Verwendung von ONTAP Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit

Bei der Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit sind bestimmte Einschränkungen zu beachten.

- Die `vserver security file-directory`Befehlsfamilie unterstützt das Festlegen von NFSv4-ACLs nicht.

  NTFS-Sicherheitsdeskriptoren können nur auf NTFS-Dateien und -Ordner angewendet werden.

Sicherheitsdeskriptoren werden verwendet, um die ONTAP SMB Datei- und Ordnersicherheit anzuwenden.

Sicherheitsdeskriptoren enthalten die Zugriffskontrolllisten, die festlegen, welche Aktionen ein Benutzer an Dateien und Ordnern durchführen kann und was protokolliert wird, wenn ein Benutzer auf Dateien und Ordner zugreift.

- **Berechtigungen**

  Berechtigungen werden vom Besitzer eines Objekts erteilt oder verweigert und bestimmen, welche Aktionen ein Objekt (Benutzer, Gruppen oder Computerobjekte) für bestimmte Dateien oder Ordner ausführen kann.

- **Sicherheitsdeskriptoren**

  Sicherheitsdeskriptoren sind Datenstrukturen, die Sicherheitsinformationen enthalten, die die Berechtigungen für eine Datei oder einen Ordner definieren.

- **Zugriffskontrolllisten (ACLs)**

  Zugriffssteuerungslisten (ACLs) sind Listen innerhalb eines Sicherheitsdeskriptors, die Informationen darüber enthalten, welche Aktionen Benutzer, Gruppen oder Computerobjekte für die Datei oder den Ordner ausführen dürfen, auf den der Sicherheitsdeskriptor angewendet wird. Der Sicherheitsdeskriptor kann die folgenden zwei Arten von ACLs enthalten:

  - Diskretionäre Zugriffskontrolllisten (DACLs)
  - Systemzugriffskontrolllisten (SACLs)

- **Diskretionäre Zugriffskontrolllisten (DACLs)**

  DACLs enthalten die Liste der SIDS für die Benutzer, Gruppen und Computerobjekte, denen der Zugriff auf Dateien oder Ordner erlaubt oder verweigert wird. DACLs enthalten null oder mehr Zugriffssteuerungseinträge (ACEs).

- **Systemzugriffskontrolllisten (SACLs)**

  SACLs enthalten die Liste der SIDS für die Benutzer, Gruppen und Computerobjekte, für die erfolgreiche oder fehlgeschlagene Überwachungsereignisse protokolliert werden. SACLs enthalten null oder mehr Zugriffssteuerungseinträge (ACEs).

- **Zugriffskontrolleinträge (ACEs)**

  ACEs sind einzelne Einträge entweder in DACLs oder SACLs:

  - Ein DACL-Zugriffskontrolleintrag legt die Zugriffsrechte fest, die für bestimmte Benutzer, Gruppen oder Computerobjekte erlaubt oder verweigert werden.
  - Ein SACL-Zugriffskontrolleintrag gibt an, welche Erfolgs- oder Fehlerereignisse beim Überwachen bestimmter Aktionen von bestimmten Benutzern, Gruppen oder Computerobjekten protokolliert werden.

- **Berechtigungsvererbung**

  Die Berechtigungsvererbung beschreibt, wie Berechtigungen, die in Sicherheitsdeskriptoren definiert sind, von einem übergeordneten Objekt auf ein Objekt übertragen werden. Nur vererbbare Berechtigungen werden von untergeordneten Objekten übernommen. Beim Festlegen von Berechtigungen für das übergeordnete Objekt kann festgelegt werden, ob Ordner, Unterordner und Dateien diese mit „Apply to `this-folder`, `sub-folders` und `files`“ erben können.

Verwandte Informationen

- "SMB und NFS Auditierung und Sicherheitsverfolgung"
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner

Informationen zur Anwendung von Dateiverzeichnisrichtlinien, die lokale SMB-Benutzer oder -Gruppen auf dem ONTAP SVM Disaster Recovery-Ziel verwenden

Bestimmte Richtlinien sind zu beachten, bevor Dateiverzeichnisrichtlinien auf der Storage Virtual Machine (SVM) Disaster Recovery Ziel in einer ID Discard Konfiguration angewendet werden, wenn die Dateiverzeichnisrichtlinienkonfiguration lokale Benutzer oder Gruppen entweder im Sicherheitsdeskriptor oder in den DACL- oder SACL-Einträgen verwendet.

Eine Disaster Recovery-Konfiguration kann für eine SVM eingerichtet werden, bei der die Quell-SVM im Quell-Cluster die Daten und die Konfiguration von der Quell-SVM auf eine Ziel-SVM in einem Ziel-Cluster repliziert.

Es stehen zwei Arten der SVM-Notfallwiederherstellung zur Verfügung:

- Identität gewahrt

  Bei dieser Konfiguration bleibt die Identität der SVM und des CIFS-Servers erhalten.

- Identität verworfen

  Bei dieser Konfiguration bleibt die Identität der SVM und des CIFS-Servers nicht erhalten. In diesem Szenario unterscheiden sich die Namen der SVM und des CIFS-Servers auf der Ziel-SVM von den Namen der SVM und des CIFS-Servers auf der Quell-SVM.

Richtlinien für verworfene Identitätskonfigurationen

In einer Konfiguration mit verworfener Identität muss für eine SVM-Quelle, die lokale Benutzer-, Gruppen- und Berechtigungskonfigurationen enthält, der Name der lokalen Domäne (lokaler CIFS-Servername) so geändert werden, dass er mit dem CIFS-Servernamen auf der SVM-Ziel übereinstimmt. Beispielsweise, wenn der Name der Quell-SVM „vs1“ und der CIFS-Servername „CIFS1“ ist, und der Name der Ziel-SVM „vs1_dst“ und der CIFS-Servername „CIFS1_DST“ ist, wird der lokale Domänenname für einen lokalen Benutzer mit dem Namen „CIFS1\user1“ auf der Ziel-SVM automatisch in „CIFS1_DST\user1“ geändert:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Obwohl lokale Benutzer- und Gruppennamen in den lokalen Benutzer- und Gruppendatenbanken automatisch geändert werden, werden lokale Benutzer- oder Gruppennamen in Dateiverzeichnisrichtlinienkonfigurationen (Richtlinien, die auf der CLI mit der `vserver security file-directory` Befehlfamilie konfiguriert werden) nicht automatisch geändert.

Wenn beispielsweise für “vs1” ein DACL-Eintrag konfiguriert wurde, bei dem der `-account` Parameter auf “CIFS1\user1” gesetzt ist, wird die Einstellung auf der Ziel-SVM nicht automatisch geändert, um den Namen des CIFS-Servers des Ziels widerzuspiegeln.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Es sind die `vserver security file-directory modify` Befehle zu verwenden, um den CIFS-Server-Namen manuell in den Namen des Ziel CIFS-Servers zu ändern.

Datei Verzeichnis-Richtlinienkonfigurationskomponenten, die Kontoparameter enthalten

Es gibt drei Konfigurationskomponenten für Datei-Verzeichnisrichtlinien, die Parametereinstellungen verwenden können, die lokale Benutzer oder Gruppen enthalten können:

- Sicherheitsdeskriptor

  Optional kann der Besitzer des Sicherheitsdeskriptors und die primäre Gruppe des Besitzers des Sicherheitsdeskriptors angegeben werden. Wenn der Sicherheitsdeskriptor einen lokalen Benutzer oder eine lokale Gruppe für die Einträge Besitzer und primäre Gruppe verwendet, muss der Sicherheitsdeskriptor so geändert werden, dass im Kontonamen die Ziel-SVM verwendet wird. Mit dem `vserver security file-directory ntfs modify` Befehl können alle erforderlichen Änderungen an den Kontonamen vorgenommen werden.

- DACL-Einträge

  Jeder DACL-Eintrag muss einem Konto zugeordnet sein. Alle DACLs, die lokale Benutzer- oder

Gruppenkonten verwenden, sind so zu ändern, dass sie den Ziel-SVM-Namen verwenden. Da der Kontoname für bestehende DACL-Einträge nicht geändert werden kann, sind alle DACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren zu entfernen, neue DACL-Einträge mit den korrigierten Zielkontonamen zu erstellen und diese neuen DACL-Einträge den entsprechenden Sicherheitsdeskriptoren zuzuordnen.

- SACL-Einträge

  Jeder SACL-Eintrag muss einem Konto zugeordnet sein. Alle SACLs, die lokale Benutzer- oder Gruppenkonten verwenden, sind so zu ändern, dass sie den Ziel-SVM-Namen verwenden. Da der Kontoname für bestehende SACL-Einträge nicht geändert werden kann, sind alle SACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren zu entfernen, neue SACL-Einträge mit den korrigierten Zielkontonamen zu erstellen und diese neuen SACL-Einträge den entsprechenden Sicherheitsdeskriptoren zuzuordnen.

Alle notwendigen Änderungen an den lokalen Benutzern oder Gruppen, die in der Dateiverzeichnisrichtlinienkonfiguration verwendet werden, sind vorzunehmen, bevor die Richtlinie angewendet wird; andernfalls schlägt der Anwendungsvorgang fehl.

Dateisicherheit für NTFS-Dateien und Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden

Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern

Das Erstellen eines NTFS-Sicherheitsdeskriptors (Dateisicherheitsrichtlinie) ist der erste Schritt beim Konfigurieren und Anwenden von NTFS-Zugriffssteuerungslisten (ACLs) auf Dateien und Ordner innerhalb von Storage Virtual Machines (SVMs). Der Sicherheitsdeskriptor kann in einer Richtlinienaufgabe dem Datei- oder Ordnerpfad zugeordnet werden.

Über diese Aufgabe

Sie können NTFS-Sicherheitsdeskriptoren für Dateien und Ordner erstellen, die sich in NTFS-Sicherheitsstil-Volumes befinden, oder für Dateien und Ordner, die sich auf Volumes mit gemischtem Sicherheitsstil befinden.

Standardmäßig werden beim Erstellen eines Sicherheitsdeskriptors vier Einträge in der diskretionären Zugriffssteuerungsliste (DACL-ACEs) zu diesem Sicherheitsdeskriptor hinzugefügt. Die vier Standard-ACEs sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Wo die Berechtigungen angewendet werden
BUILTIN\Administratoren	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
BUILTIN\Users	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
ERSTELLER-BESITZER	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Eigentümer des Sicherheitsdeskriptors
- Primärgruppe des Eigentümers
- Rohsteuer-Flags

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen befinden sich in der "ONTAP-Befehlsreferenz".

NTFS-DACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen

Das Hinzufügen von DACL (discretionary access control list) Zugriffssteuerungsliste-Zugriffssteuerungseinträgen (ACEs) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Konfiguration und Anwendung von NTFS-ACLs auf eine Datei oder einen Ordner. Jeder Eintrag legt fest, welchem Objekt der Zugriff erlaubt oder verweigert wird, und definiert, was das Objekt mit den in der ACE definierten Dateien oder Ordnern tun darf oder nicht tun darf.

Über diese Aufgabe

Der DACL des Sicherheitsdeskriptors kann um eine oder mehrere ACEs ergänzt werden.

Enthält der Sicherheitsdeskriptor eine DACL mit bereits vorhandenen ACEs, wird die neue ACE der DACL hinzugefügt. Enthält der Sicherheitsdeskriptor keine DACL, wird die DACL erstellt und die neue ACE hinzugefügt.

Sie können DACL-Einträge optional anpassen, indem Sie festlegen, welche Rechte Sie für das im `-account` Parameter angegebene Konto erlauben oder verweigern möchten. Es gibt drei sich gegenseitig ausschließende Methoden zur Angabe von Rechten:

- Rechte
- Erweiterte Rechte
- Rohrechte (erweiterte Berechtigung)

> Wenn Sie keine Rechte für den DACL-Eintrag angeben, werden die Rechte standardmäßig auf `Full Control` gesetzt.

DACL-Einträge lassen sich optional anpassen, indem festgelegt wird, wie die Vererbung angewendet wird.

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einen DACL-Eintrag zu einem Sicherheitsdeskriptor hinzufügen: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Es sollte überprüft werden, ob der DACL-Eintrag korrekt ist: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type`

```
{allow|deny} -account name_or_SID

vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
                Vserver: vs1
Security Descriptor Name: sd1
           Allow or Deny: deny
     Account Name or SID: DOMAIN\joe
           Access Rights: full-control
  Advanced Access Rights: -
                Apply To: this-folder
           Access Rights: full-control
```

Weitere Informationen zu `vserver security file-directory ntfs dacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB Sicherheitsrichtlinien erstellen

Das Erstellen einer Dateisicherheitsrichtlinie für SVMs ist der dritte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf eine Datei oder einen Ordner. Eine Richtlinie dient als Container für verschiedene Aufgaben, wobei jede Aufgabe einen einzelnen Eintrag darstellt, der auf Dateien oder Ordner angewendet werden kann. Aufgaben können der Sicherheitsrichtlinie später hinzugefügt werden.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollte die Sicherheitsrichtlinie mit jedem SVM (das NTFS-Sicherheitsstil-Volumes oder gemischte Sicherheitsstil-Volumes enthält) verknüpft werden.

Schritte

1. Eine Sicherheitsrichtlinie erstellen: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver
   vs1
   ```

2. Die Sicherheitsrichtlinie wird überprüft: `vserver security file-directory policy show`

   ```
   vserver security file-directory policy show
     Vserver          Policy Name
    ------------     --------------
       vs1              policy1
   ```

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe wird diese einer Sicherheitsrichtlinie zugeordnet. Einer Sicherheitsrichtlinie können ein oder mehrere Aufgabeneinträge hinzugefügt werden.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf eine einzelne Operation, die von einer Sicherheitsrichtlinie an Dateien oder Ordnern mit NTFS- oder gemischter Sicherheit (oder an einem Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Dient zur Festlegung von Aufgaben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. Über Datei- und Verzeichnisaufgaben angewendete ACLs können mit SMB-Clients oder der ONTAP CLI verwaltet werden.

- Storage-Level Access Guard Aufgaben

  Dient zur Angabe von Aufgaben, die Storage-Level Access Guard-Sicherheitsdeskriptoren auf ein bestimmtes Volume anwenden. ACLs, die durch Storage-Level Access Guard-Aufgaben angewendet werden, können nur über die ONTAP CLI verwaltet werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder einer Gruppe von Dateien (oder Ordnern). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Innerhalb einer Richtlinie kann es pro Pfad nur eine Aufgabe geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10.000 Aufgabeneinträge vorhanden sein.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Auch wenn eine Richtlinie mehr als eine Aufgabe enthalten kann, kann eine Richtlinie nicht so konfiguriert werden, dass sie sowohl Aufgaben für Dateiverzeichnisse als auch Storage-Level Access Guard-Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

Beim Hinzufügen von Aufgaben zu Sicherheitsrichtlinien müssen die folgenden vier erforderlichen Parameter angegeben werden:

- SVM-Name
- Richtlinienname
- Pfad

- Sicherheitsdeskriptor, der dem Pfad zugeordnet wird

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Zugriffskontrolltyp

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einer Sicherheitsrichtlinie wird eine Aufgabe mit zugehörigem Sicherheitsdeskriptor hinzugefügt: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` ist der Standardwert für den `-access-control` Parameter. Die Angabe des Zugriffskontrolltyps bei der Konfiguration von Datei- und Verzeichniszugriffsaufgaben ist optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Die Konfiguration der Richtlinienaufgabe überprüfen: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB-Sicherheitsrichtlinien anwenden

Das Anwenden einer Dateisicherheitsrichtlinie auf SVMs ist der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie definierten Sicherheitseinstellungen auf NTFS-Dateien und -Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder gemischter Sicherheitsstil).

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Beim Anwenden einer Sicherheitsrichtlinie und der zugehörigen DACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Schritt

1. Eine Sicherheitsrichtlinie anwenden: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   Der Auftrag zur Anwendung der Richtlinie wird eingeplant und die Job-ID wird zurückgegeben.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 –id
   53322" command to view the status of the operation
   ```

ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen

Beim Anwenden der Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) kann der Fortschritt der Aufgabe überwacht werden, indem der Sicherheitsrichtlinienauftrag überwacht wird. Dies ist hilfreich, wenn festgestellt werden soll, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn ein lang andauernder Auftrag vorliegt, bei dem eine Sicherheitsrichtlinie auf eine große Anzahl von Dateien und Ordnern angewendet wird.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienauftrag anzuzeigen, sollte der `-instance` Parameter verwendet werden.

Schritt

1. Der Auftrag zur Sicherheitsrichtlinie wird überwacht: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Die Sicherheit von ONTAP SMB-Dateien überprüfen

Sie können die Dateisicherheitseinstellungen überprüfen, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die Sie die Sicherheitsrichtlinie angewendet haben, die gewünschten Einstellungen aufweisen.

Über diese Aufgabe

Sie müssen den Namen der SVM, die die Daten enthält, sowie den Pfad zu den Dateien und Ordnern angeben, deren Sicherheitseinstellungen überprüft werden sollen. Der optionale `-expand-mask`Parameter kann verwendet werden, um detaillierte Informationen zu den Sicherheitseinstellungen anzuzeigen.

Schritt

1. Datei- und Ordnersicherheitseinstellungen anzeigen: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   -expand-mask true
   ```

   ```
            Vserver: vs1
                 File Path: /data/engineering
         File Inode Number: 5544
            Security Style: ntfs
           Effective Style: ntfs
            DOS Attributes: 10
    DOS Attributes in Text: ----D---
   Expanded Dos Attributes: 0x10
        ...0 .... .... .... = Offline
        .... ..0. .... .... = Sparse
        .... .... 0... .... = Normal
        .... .... ..0. .... = Archive
        .... .... ...1 .... = Directory
        .... .... .... .0.. = System
        .... .... .... ..0. = Hidden
        .... .... .... ...0 = Read Only
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0x8004

                                1... .... .... .... = Self Relative
                                .0.. .... .... .... = RM Control Valid
                                ..0. .... .... .... = SACL Protected
                                ...0 .... .... .... = DACL Protected
                                .... 0... .... .... = SACL Inherited
                                .... .0.. .... .... = DACL Inherited
   ```

```
                            .... ..0. .... .... = SACL Inherit Required
                            .... ...0 .... .... = DACL Inherit Required
                            .... .... ..0. .... = SACL Defaulted
                            .... .... ...0 .... = SACL Present
                            .... .... .... 0... = DACL Defaulted
                            .... .... .... .1.. = DACL Present
                            .... .... .... ..0. = Group Defaulted
                            .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
```

```
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...1 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...0 .... .... .... .... .... =
Synchronize
                            .... .... .... 0... .... .... .... .... =
Write Owner
                            .... .... .... .0.. .... .... .... .... =
Write DAC
                            .... .... .... ..0. .... .... .... .... =
Read Control
                            .... .... .... ...0 .... .... .... .... =
Delete
                            .... .... .... .... .... ...0 .... .... =
Write Attributes
                            .... .... .... .... .... .... 0... .... =
Read Attributes
                            .... .... .... .... .... .... .0.. .... =
Delete Child
                            .... .... .... .... .... .... ..0. .... =
Execute
                            .... .... .... .... .... .... ...0 .... =
Write EA
                            .... .... .... .... .... .... .... 0... =
Read EA
                            .... .... .... .... .... .... .... .0.. =
Append
                            .... .... .... .... .... .... .... ..0. =
Write
                            .... .... .... .... .... .... .... ...0 =
Read
```

Überwachungsrichtlinien für NTFS-Dateien und -Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden

ONTAP Befehle zum Konfigurieren und Anwenden von SMB-Überwachungsrichtlinien auf NTFS-Dateien und Ordner

Es sind mehrere Schritte erforderlich, um Überwachungsrichtlinien auf NTFS-Dateien und -Ordner mit der ONTAP CLI anzuwenden. Zuerst wird ein NTFS-Sicherheitsdeskriptor erstellt und SACLs zu diesem Sicherheitsdeskriptor hinzugefügt. Anschließend wird eine Sicherheitsrichtlinie erstellt und Richtlinienaufgaben hinzugefügt. Danach wird die Sicherheitsrichtlinie auf eine Storage Virtual Machine (SVM) angewendet.

Über diese Aufgabe

Nach der Anwendung der Sicherheitsrichtlinie können Sie den Sicherheitsrichtlinienauftrag überwachen und anschließend die Einstellungen für die angewendete Audit-Richtlinie überprüfen.

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Verwandte Informationen

- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard
- Informationen zu den Grenzen bei der Verwendung von Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit
- Sicherheitsdeskriptoren werden verwendet, um die Sicherheit von Dateien und Ordnern festzulegen.
- "SMB und NFS Auditierung und Sicherheitsverfolgung"
- NTFS-Sicherheitsdeskriptoren auf Servern erstellen

Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern

Das Erstellen einer NTFS-Sicherheitsdeskriptor-Überwachungsrichtlinie ist der erste Schritt beim Konfigurieren und Anwenden von NTFS-Zugriffssteuerungslisten (ACLs) auf Dateien und Ordner in SVMs. Der Sicherheitsdeskriptor wird dem Datei- oder Ordnerpfad in einer Richtlinienaufgabe zugeordnet.

Über diese Aufgabe

Sie können NTFS-Sicherheitsdeskriptoren für Dateien und Ordner erstellen, die sich in NTFS-Sicherheitsstil-Volumes befinden, oder für Dateien und Ordner, die sich auf Volumes mit gemischtem Sicherheitsstil befinden.

Standardmäßig werden beim Erstellen eines Sicherheitsdeskriptors vier Einträge in der diskretionären Zugriffssteuerungsliste (DACL-ACEs) zu diesem Sicherheitsdeskriptor hinzugefügt. Die vier Standard-ACEs sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Wo die Berechtigungen angewendet werden
BUILTIN\Administratoren	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien

Objekt	Zugriffstyp	Zugriffsrechte	Wo die Berechtigungen angewendet werden
BUILTIN\Users	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
ERSTELLER-BESITZER	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Eigentümer des Sicherheitsdeskriptors
- Primärgruppe des Eigentümers
- Rohsteuer-Flags

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Wenn Sie die erweiterten Parameter verwenden möchten, die Berechtigungsstufe auf „Erweitert“ setzen: `set -privilege advanced`
2. Ein Sicherheitsdeskriptor wird erstellt: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. Es sollte überprüft werden, ob die Konfiguration des Sicherheitsdeskriptors korrekt ist: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Wenn Sie sich auf der erweiterten Berechtigungsebene befinden, zur Administrator-Berechtigungsebene zurückkehren: `set -privilege admin`

NTFS-SACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen

Das Hinzufügen von SACL (system access control list) Zugriffssteuerungsliste-Zugriffskontrolleinträgen (ACEs) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt beim Erstellen von NTFS-Überwachungsrichtlinien für Dateien oder Ordner in SVMs.

Jeder Eintrag identifiziert den Benutzer oder die Gruppe, die überwacht werden soll. Der SACL-Eintrag definiert, ob erfolgreiche oder fehlgeschlagene Zugriffsversuche protokolliert werden sollen.

Über diese Aufgabe

Der SACL des Sicherheitsdeskriptors kann um eine oder mehrere ACEs ergänzt werden.

Enthält der Sicherheitsdeskriptor eine SACL mit bereits vorhandenen ACEs, wird die neue ACE der SACL hinzugefügt. Enthält der Sicherheitsdeskriptor keine SACL, wird die SACL erstellt und die neue ACE hinzugefügt.

Sie können SACL-Einträge konfigurieren, indem Sie festlegen, welche Rechte für erfolgreiche oder fehlgeschlagene Ereignisse für das im `-account` Parameter angegebene Konto geprüft werden sollen. Es gibt drei sich gegenseitig ausschließende Methoden zur Angabe von Rechten:

- Rechte
- Erweiterte Rechte
- Rohrechte (erweiterte Berechtigung)

Wenn Sie keine Rechte für den SACL-Eintrag angeben, ist die Standardeinstellung `Full Control`.

Sie können SACL-Einträge optional anpassen, indem Sie festlegen, wie die Vererbung mit dem `apply to` Parameter angewendet wird. Wenn Sie diesen Parameter nicht angeben, wird der SACL-Eintrag standardmäßig auf diesen Ordner, Unterordner und Dateien angewendet.

Schritte

1. Einen SACL-Eintrag zu einem Sicherheitsdeskriptor hinzufügen: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Es sollte überprüft werden, ob der SACL-Eintrag korrekt ist: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                   Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                    Advanced Access Rights: -
                                  Apply To: this-folder
   ```

```
                                    Access Rights: full-control
```

ONTAP SMB Sicherheitsrichtlinien erstellen

Das Erstellen einer Überwachungsrichtlinie für Storage Virtual Machines (SVMs) ist der dritte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten (ACLs) auf eine Datei oder einen Ordner. Eine Richtlinie dient als Container für verschiedene Aufgaben, wobei jede Aufgabe einen einzelnen Eintrag darstellt, der auf Dateien oder Ordner angewendet werden kann. Aufgaben können der Sicherheitsrichtlinie später hinzugefügt werden.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollte die Sicherheitsrichtlinie mit jeder Storage Virtual Machine (SVM) (die NTFS-Sicherheitsstil-Volumes oder gemischte Sicherheitsstil-Volumes enthält) verknüpft werden.

Schritte

1. Eine Sicherheitsrichtlinie erstellen: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver vs1
   ```

2. Die Sicherheitsrichtlinie wird überprüft: `vserver security file-directory policy show`

   ```
   vserver security file-directory policy show
      Vserver           Policy Name
    ------------      --------------
        vs1               policy1
   ```

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe wird diese einer Sicherheitsrichtlinie zugeordnet. Einer Sicherheitsrichtlinie können ein oder mehrere Aufgabeneinträge hinzugefügt werden.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf eine einzelne Operation, die von einer Sicherheitsrichtlinie an Dateien oder Ordnern mit NTFS- oder gemischter Sicherheit (oder an einem Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Dient zur Festlegung von Aufgaben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. Über Datei- und Verzeichnisaufgaben angewendete ACLs können mit SMB-Clients oder der ONTAP CLI verwaltet werden.

- Storage-Level Access Guard Aufgaben

  Dient zur Angabe von Aufgaben, die Storage-Level Access Guard-Sicherheitsdeskriptoren auf ein bestimmtes Volume anwenden. ACLs, die durch Storage-Level Access Guard-Aufgaben angewendet werden, können nur über die ONTAP CLI verwaltet werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder einer Gruppe von Dateien (oder Ordnern). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Innerhalb einer Richtlinie kann es pro Pfad nur eine Aufgabe geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10.000 Aufgabeneinträge vorhanden sein.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Auch wenn eine Richtlinie mehr als eine Aufgabe enthalten kann, kann eine Richtlinie nicht so konfiguriert werden, dass sie sowohl Aufgaben für Dateiverzeichnisse als auch Storage-Level Access Guard-Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Zugriffskontrolltyp

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einer Sicherheitsrichtlinie wird eine Aufgabe mit zugehörigem Sicherheitsdeskriptor hinzugefügt: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` ist der Standardwert für den `-access-control` Parameter. Die Angabe des Zugriffskontrolltyps bei der Konfiguration von Datei- und Verzeichniszugriffsaufgaben ist optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Die Konfiguration der Richtlinienaufgabe überprüfen: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB-Sicherheitsrichtlinien anwenden

Das Anwenden einer Überwachungsrichtlinie auf SVMs ist der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie definierten Sicherheitseinstellungen auf NTFS-Dateien und -Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder gemischter Sicherheitsstil).

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Beim Anwenden einer Sicherheitsrichtlinie und der zugehörigen DACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Schritt

1. Eine Sicherheitsrichtlinie anwenden: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   Der Auftrag zur Anwendung der Richtlinie wird eingeplant und die Job-ID wird zurückgegeben.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen

Beim Anwenden der Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) kann der Fortschritt der Aufgabe überwacht werden, indem der Sicherheitsrichtlinienauftrag überwacht wird. Dies ist hilfreich, wenn festgestellt werden soll, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn ein lang andauernder Auftrag vorliegt, bei dem eine Sicherheitsrichtlinie auf eine große Anzahl von Dateien und Ordnern angewendet wird.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienauftrag anzuzeigen, sollte der `-instance` Parameter verwendet werden.

Schritt

1. Der Auftrag zur Sicherheitsrichtlinie wird überwacht: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

ONTAP SMB Auditrichtlinien überprüfen

Die Überwachungsrichtlinie kann überprüft werden, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die die Sicherheitsrichtlinie angewendet wurde, die gewünschten Überwachungssicherheitseinstellungen aufweisen.

Über diese Aufgabe

Sie verwenden den `vserver security file-directory show` Befehl, um Informationen zur Überwachungsrichtlinie anzuzeigen. Es muss der Name der SVM, die die Daten enthält, sowie der Pfad zu den Daten angegeben werden, deren Datei- oder Ordner-Überwachungsrichtlinieninformationen angezeigt werden sollen.

Schritt

1. Einstellungen für die Überwachungsrichtlinie anzeigen: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Beispiel

Der folgende Befehl zeigt die auf den Pfad “/corp” in SVM vs1 angewendeten Überwachungsrichtlinieninformationen an. Auf den Pfad sind sowohl ein SUCCESS- als auch ein SUCCESS/FAIL-SACL-Eintrag angewendet:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
```

```
                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Informationen zur Verwaltung von ONTAP SMB-Sicherheitsrichtlinienjobs

Wenn ein Sicherheitsrichtlinienauftrag existiert, kann unter bestimmten Umständen diese Sicherheitsrichtlinie oder die der Richtlinie zugewiesenen Aufgaben nicht geändert werden. Es ist wichtig zu verstehen, unter welchen Bedingungen Sicherheitsrichtlinien geändert werden können oder nicht, damit etwaige Änderungsversuche erfolgreich sind. Zu den Änderungen an der Richtlinie zählen das Hinzufügen, Entfernen oder Ändern von Aufgaben, die der Richtlinie zugewiesen sind, sowie das Löschen oder Ändern der Richtlinie.

Sie können eine Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe nicht ändern, wenn ein Auftrag für diese Richtlinie existiert und sich dieser Auftrag in einem der folgenden Zustände befindet:

- Der Auftrag wird ausgeführt oder ist in Bearbeitung.
- Der Auftrag ist pausiert.
- Der Auftrag wird fortgesetzt und befindet sich im Status „Wird ausgeführt“.
- Wenn der Job auf das Failover zu einem anderen Knoten wartet.

Unter den folgenden Umständen ist es möglich, eine Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe erfolgreich zu ändern, sofern ein Auftrag für eine Sicherheitsrichtlinie existiert:

- Der Policy Job wurde gestoppt.

- Der Policy-Job wurde erfolgreich abgeschlossen.

ONTAP Befehle zur Verwaltung von NTFS- und SMB-Sicherheitsrichtlinien und Zugriffskontrolleinträgen

Mit ONTAP-Befehlen können Sie NTFS-Sicherheitsdeskriptoren und Zugriffssteuerungseinträge (ACEs) in DACLs und SACLs erstellen, ändern, löschen und Informationen dazu anzeigen. Sie können auch ONTAP-Befehle verwenden, um SMB-Sicherheitsrichtlinien, Richtlinienaufgaben und Richtlinienaufträge zu verwalten.

ONTAP Befehle zur Verwaltung von NTFS-Sicherheitsdeskriptoren auf SMB-Servern

Für die Verwaltung von Sicherheitsdeskriptoren stehen spezielle ONTAP Befehle zur Verfügung. Sie können Sicherheitsdeskriptoren erstellen, ändern, löschen und Informationen darüber anzeigen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NTFS-Sicherheitsdeskriptoren erstellen	`vserver security file-directory ntfs create`
Vorhandene NTFS-Sicherheitsdeskriptoren ändern	`vserver security file-directory ntfs modify`
Informationen zu vorhandenen NTFS-Sicherheitsdeskriptoren anzeigen	`vserver security file-directory ntfs show`
NTFS-Sicherheitsdeskriptoren löschen	`vserver security file-directory ntfs delete`

Weitere Informationen zu `vserver security file-directory ntfs` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NTFS DACL-Zugriffskontrolleinträgen auf SMB-Servern

Für die Verwaltung von DACL-Zugriffskontrolleinträgen (ACEs) stehen spezielle ONTAP Befehle zur Verfügung. Es ist möglich, ACEs jederzeit zu NTFS DACLs hinzuzufügen. Auch die Verwaltung bestehender NTFS DACLs durch Ändern, Löschen und Anzeigen von Informationen zu ACEs in DACLs ist möglich.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
ACEs erstellen und zu NTFS-DACLs hinzufügen	`vserver security file-directory ntfs dacl add`
Vorhandene ACEs in NTFS-DACLs ändern	`vserver security file-directory ntfs dacl modify`
Informationen zu vorhandenen ACEs in NTFS-DACLs	`vserver security file-directory ntfs dacl show`
Vorhandene ACEs aus NTFS-DACLs entfernen	`vserver security file-directory ntfs dacl remove`

Weitere Informationen zu `vserver security file-directory ntfs dacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NTFS SACL-Zugriffskontrolleinträgen auf SMB-Servern

Für die Verwaltung von SACL-Zugriffskontrolleinträgen (ACEs) stehen spezielle ONTAP Befehle zur Verfügung. ACEs können jederzeit zu NTFS SACLs hinzugefügt werden. Auch die Verwaltung bestehender NTFS SACLs durch Ändern, Löschen und Anzeigen von Informationen zu ACEs in SACLs ist möglich.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
ACEs erstellen und zu den NTFS-SACLs hinzufügen	`vserver security file-directory ntfs sacl add`
Vorhandene ACEs in NTFS-SACLs ändern	`vserver security file-directory ntfs sacl modify`
Informationen zu vorhandenen ACEs in NTFS-SACLs anzeigen	`vserver security file-directory ntfs sacl show`
Vorhandene ACEs aus den NTFS-SACLs entfernen	`vserver security file-directory ntfs sacl remove`

Weitere Informationen zu `vserver security file-directory ntfs sacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinien

Für die Verwaltung von Sicherheitsrichtlinien stehen spezielle ONTAP Befehle zur Verfügung. Es können Informationen zu Richtlinien angezeigt und Richtlinien gelöscht werden. Eine Sicherheitsrichtlinie kann nicht geändert werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinien erstellen	`vserver security file-directory policy create`
Informationen zu Sicherheitsrichtlinien	`vserver security file-directory policy show`
Sicherheitsrichtlinien löschen	`vserver security file-directory policy delete`

Weitere Informationen zu `vserver security file-directory policy` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinienaufgaben

Es gibt ONTAP Befehle zum Hinzufügen, Ändern, Entfernen und Anzeigen von Informationen über Aufgaben von Sicherheitsrichtlinien.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinienaufgaben hinzufügen	`vserver security file-directory policy task add`
Aufgaben zur Änderung der Sicherheitsrichtlinie	`vserver security file-directory policy task modify`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu Aufgaben der Sicherheitsrichtlinie	`vserver security file-directory policy task show`
Sicherheitsrichtlinien-Aufgaben entfernen	`vserver security file-directory policy task remove`

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB Security Policy Jobs

Es gibt ONTAP Befehle zum Anhalten, Fortsetzen, Stoppen und Anzeigen von Informationen über Sicherheitsrichtlinienaufträge.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinien-Jobs pausieren	`vserver security file-directory job pause -vserver vserver_name -id integer`
Sicherheitsrichtlinien-Jobs fortsetzen	`vserver security file-directory job resume -vserver vserver_name -id integer`
Informationen zu Sicherheitsrichtlinien-Jobs anzeigen	`vserver security file-directory job show -vserver vserver_name`Die Job-ID eines Jobs lässt sich mit diesem Befehl ermitteln.
Sicherheitsrichtlinien-Jobs stoppen	`vserver security file-directory job stop -vserver vserver_name -id integer`

Weitere Informationen zu `vserver security file-directory job` finden sich in der "ONTAP-Befehlsreferenz".

Den Metadatencache für SMB-Freigaben konfigurieren

Metadaten-Caching ermöglicht das Zwischenspeichern von Dateiattributen auf SMB 1.0 Clients, um einen schnelleren Zugriff auf Datei- und Ordnerattribute zu bieten. Das Attribut-Caching kann für jede Freigabe einzeln aktiviert oder deaktiviert werden. Die Gültigkeitsdauer (Time-to-Live) der zwischengespeicherten Einträge kann ebenfalls konfiguriert werden, wenn Metadaten-Caching aktiviert ist. Eine Konfiguration des Metadaten-Cachings ist nicht erforderlich, wenn Clients über SMB 2.x oder SMB 3.0 auf Freigaben zugreifen.

Wenn diese Funktion aktiviert ist, speichert der SMB-Metadatencache Pfad- und Dateiattributdaten für eine begrenzte Zeit. Dies kann die SMB-Leistung für SMB 1.0 Clients mit gängigen Arbeitslasten verbessern.

Bei bestimmten Aufgaben erzeugt SMB ein erhebliches Datenaufkommen, das mehrere identische Abfragen für Pfad- und Dateimetadaten enthalten kann. Die Anzahl redundanter Abfragen lässt sich reduzieren und die Leistung für SMB 1.0 Clients verbessern, wenn SMB-Metadaten-Caching verwendet wird, um die Informationen stattdessen aus dem Cache abzurufen.

Es ist zwar unwahrscheinlich, aber möglich, dass der Metadaten-Cache veraltete Informationen

an SMB 1.0-Clients ausliefert. Falls dieses Risiko in Ihrer Umgebung nicht akzeptabel ist, sollte diese Funktion nicht aktiviert werden.

Der ONTAP SMB-Metadaten-Cache kann aktiviert werden.

Die SMB-Leistung für SMB 1.0-Clients lässt sich durch Aktivierung des SMB-Metadaten-Caches verbessern. Standardmäßig ist die SMB-Metadaten-Zwischenspeicherung deaktiviert.

Schritt

1. Aktivieren Sie das SMB-Metadaten-Caching für eine neue oder bestehende Freigabe:
   - Aktivieren Sie das SMB-Metadaten-Caching beim Erstellen einer neuen Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name
<share_name> -path <path> -share-properties attributecache
```

   - Aktivieren Sie das SMB-Metadaten-Caching für eine vorhandene Freigabe:

```
vserver cifs share properties add -vserver <SVM_name> -share-name
<share_name> -share-properties attributecache
```

Die Lebensdauer von ONTAP SMB Metadaten-Cache-Einträgen konfigurieren

Sie können die Lebensdauer von SMB-Metadaten-Cache-Einträgen konfigurieren, um die Leistung des SMB-Metadaten-Caches in Ihrer Umgebung zu optimieren. Der Standardwert beträgt 10 Sekunden.

Bevor Sie beginnen

Sie müssen die SMB-Metadaten-Cache-Funktion aktiviert haben. Wenn die SMB-Metadaten-Cache-Funktion nicht aktiviert ist, wird die SMB-Cache-TTL-Einstellung nicht verwendet.

Schritt

1. Konfigurieren Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen auf einer neuen oder vorhandenen Freigabe:
   - Konfigurieren Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen beim Erstellen einer neuen Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name
<share_name> -path <path> -attribute-cache-ttl
[integerh][integerm][integers]
```

   - Konfigurieren der Lebensdauer von SMB-Metadaten-Cache-Einträgen auf einer vorhandenen Freigabe:

```
vserver cifs share modify -vserver <SVM_name> -share-name
<share_name> -attribute-cache-ttl [integerh][integerm][integers]
```

Beim Erstellen oder Ändern von Freigaben können Sie zusätzliche Konfigurationsoptionen und Eigenschaften festlegen. Weitere Informationen zu `vserver cifs share` finden sich in der "ONTAP-Befehlsreferenz".

Dateisperren verwalten

Informationen zur ONTAP SMB-Dateisperrung zwischen Protokollen

Die Dateisperrung ist eine Methode, mit der Clientanwendungen verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde. Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Handelt es sich beim Client um einen NFS-Client, sind Sperren empfehlend; handelt es sich beim Client um einen SMB-Client, sind Sperren obligatorisch.

Aufgrund von Unterschieden zwischen den Dateisperren von NFS und SMB kann es vorkommen, dass ein NFS-Client nicht auf eine Datei zugreifen kann, die zuvor von einer SMB-Anwendung geöffnet wurde.

Folgendes geschieht, wenn ein NFS-Client versucht, auf eine von einer SMB-Anwendung gesperrte Datei zuzugreifen:

- In gemischten oder NTFS-Volumes können Dateimanipulationsvorgänge wie `rm`, `rmdir` und `mv` dazu führen, dass die NFS-Anwendung fehlschlägt.
- NFS-Lese- und Schreibvorgänge werden durch die SMB-Öffnungsmodi deny-read und deny-write jeweils für lesen bzw. schreiben verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei mit einer exklusiven SMB-Bytesperre gesperrt ist.
- Link aufheben
  - Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

    Die Datei wird nach dem letzten Schließen gelöscht.
  - NFS unlink-Operationen werden nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und die Operation „Letztes Löschen beim Schließen“ für NFS nicht unterstützt wird.
  - Für UNIX-Dateisysteme wird die Operation "unlink" unterstützt.

    Es wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.
- Umbenennen
  - Für NTFS-Dateisysteme kann die Zieldatei umbenannt werden, wenn sie über SMB oder CIFS geöffnet wird.
  - NFS-Umbenennung wird nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind.

In UNIX-Sicherheitsstil-Volumes ignorieren NFS-Unlink- und Rename-Operationen den SMB-Sperrstatus und ermöglichen den Zugriff auf die Datei. Alle anderen NFS-Operationen auf UNIX-Sicherheitsstil-Volumes berücksichtigen den SMB-Sperrstatus.

Informationen zu schreibgeschützten Bits in ONTAP SMB

Das Schreibschutzbit wird für jede Datei einzeln gesetzt, um anzuzeigen, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients unter Windows können ein schreibgeschütztes Bit pro Datei setzen. NFS-Clients setzen kein schreibgeschütztes Bit pro Datei, da NFS-Clients keine Protokolloperationen haben, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann das Schreibschutzbit einer Datei setzen, wenn diese von einem SMB-Client unter Windows erstellt wird. ONTAP kann das Schreibschutzbit auch setzen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Manche Software erfordert, dass das Schreibschutzbit aktiviert ist, wenn sie von NFS-Clients und SMB-Clients verwendet wird.

Damit ONTAP die korrekten Lese- und Schreibberechtigungen für eine zwischen NFS-Client und SMB-Client gemeinsam genutzte Datei beibehält, wird das Schreibschutzbit nach den folgenden Regeln behandelt:

- NFS behandelt jede Datei, bei der das Schreibschutzbit aktiviert ist, so, als ob keine Schreibberechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Schreibberechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert war, aktiviert ONTAP das Schreibschutzbit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungsbit aktiviert, deaktiviert ONTAP das Nur-Lesen-Bit für diese Datei.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein NFS-Client versucht, die Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet; stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client, wobei die Schreibberechtigungsbits maskiert sind.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein SMB-Client das Schreibschutzbit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien, bei denen das Schreibschutzbit aktiviert ist, sind nur für root beschreibbar.

Das Schreibschutzbit interagiert mit den ACL- und Unix-Modusbits auf folgende Weise:

Wenn das Schreibschutzbit einer Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Sämtliche Unix-Modusbits, die Schreibzugriff auf die Datei ermöglichen, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber sie können sie nicht verändern.
- ACLs und UNIX-Modusbits werden zugunsten des Schreibschutzbits ignoriert. Das bedeutet, dass selbst wenn die ACL Schreibzugriff erlaubt, das Schreibschutzbit Änderungen verhindert.

Wenn das Schreibschutzbit einer Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff anhand der ACL und der UNIX-Modusbits.
  - Wenn entweder die ACL oder die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei nicht ändern.
  - Wenn weder die ACL noch die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

Änderungen an Dateiberechtigungen werden auf SMB-Clients sofort wirksam, auf NFS-Clients hingegen möglicherweise nicht sofort, wenn der NFS-Client das Attribut-Caching aktiviert.

Wie ONTAP sich von Windows bei der Handhabung von Sperren auf freigegebenen Pfadkomponenten unterscheidet

Im Gegensatz zu Windows sperrt ONTAP nicht die einzelnen Komponenten des Pfades zu einer geöffneten Datei, solange die Datei geöffnet ist. Dieses Verhalten betrifft auch SMB-Freigabepfade.

Da ONTAP die einzelnen Pfadkomponenten nicht sperrt, ist es möglich, eine Pfadkomponente oberhalb der geöffneten Datei oder Freigabe umzubenennen, was bei bestimmten Anwendungen zu Problemen führen oder den Freigabepfad in der SMB-Konfiguration ungültig machen kann. Dies kann dazu führen, dass die Freigabe nicht zugänglich ist.

Um Probleme zu vermeiden, die durch das Umbenennen von Pfadkomponenten entstehen, lassen sich Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu ONTAP SMB-Sperren anzeigen

Informationen über die aktuellen Dateisperren können angezeigt werden, einschließlich der Art der gehaltenen Sperren und des Sperrstatus, Details zu Bytebereichssperren, Sharelock-Modi, Delegation Locks und Opportunistic Locks sowie darüber, ob Sperren mit dauerhaften oder persistenten Handles geöffnet sind.

Über diese Aufgabe

Die Client-IP-Adresse kann für Sperren, die über NFSv4 oder NFSv4.1 eingerichtet wurden, nicht angezeigt werden.

Standardmäßig zeigt der Befehl Informationen zu allen Sperren an. Mit Befehlsparametern lässt sich die Anzeige von Informationen zu Sperren für eine bestimmte Storage Virtual Machine (SVM) steuern oder die Ausgabe des Befehls nach anderen Kriterien filtern.

Der `vserver locks show` Befehl zeigt Informationen über vier Arten von Sperren an:

- Byte-Range-Sperren, die nur einen Teil einer Datei sperren.
- Freigabesperren, die geöffnete Dateien sperren.
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Client-seitige Caching über NFSv4.x steuern.

Durch die Angabe optionaler Parameter lassen sich wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Informationen zu Sperren werden mit dem `vserver locks show` Befehl angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen zu einer NFSv4-Sperre für eine Datei mit dem Pfad `/vol1/file1`. Der Zugriffsmodus von Sharelock ist write-deny_none, und die Sperre wurde mit

Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte Oplock- und Sharelock-Informationen zur SMB-Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird für die Datei mit dem Sharelock-Zugriffsmodus write-deny_none an einen Client mit der IP-Adresse 10.3.1.3 gewährt. Ein Lease-Oplock wird mit dem Oplock-Level Batch gewährt:

```
cluster1::> vserver locks 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: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   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: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

```
                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              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
```

ONTAP SMB-Sperren aufheben

Wenn Dateisperren den Zugriff von Clients auf Dateien verhindern, können Informationen über die aktuell bestehenden Sperren angezeigt und anschließend bestimmte Sperren aufgehoben werden. Beispiele für Szenarien, in denen das Aufheben von Sperren erforderlich sein kann, sind das Debuggen von Anwendungen.

Über diese Aufgabe

Der `vserver locks break`Befehl ist nur auf der erweiterten Berechtigungsstufe und höher verfügbar. Weitere Informationen zu `vserver locks break` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Um die Informationen zu finden, die Sie zum Aufheben einer Sperre benötigen, verwenden Sie den `vserver locks show` Befehl.

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

2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`

3. Führen Sie eine der folgenden Aktionen aus:

Wenn ein Schloss durch Angabe von… aufgehoben werden soll	Geben Sie den Befehl ein…
Der SVM Name, der Volumenname, der LIF Name und der Dateipfad	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
Die Lock-ID	`vserver locks break -lockid UUID`

4. Zurück zur Administratorrechteebene: `set -privilege admin`

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

SMB-Aktivitäten überwachen

ONTAP SMB-Sitzungsinformationen anzeigen

Sie können Informationen zu bestehenden SMB-Sitzungen anzeigen, darunter die SMB-Verbindungs- und Sitzungs-ID sowie die IP-Adresse der Workstation, die die Sitzung nutzt. Sie können Informationen zur Protokollversion der Sitzung und zum kontinuierlich verfügbaren Schutzniveau anzeigen, was dabei hilft zu erkennen, ob die Sitzung unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefasster Form anzeigen. In vielen Fällen ist die Ausgabemenge jedoch sehr groß. Welche Informationen in der Ausgabe angezeigt werden, lässt sich durch optionale Parameter anpassen:

- Der optionale `-fields`Parameter ermöglicht die Anzeige von Ausgaben zu den ausgewählten Feldern.

  Sie können `-fields ?` eingeben, um festzustellen, welche Felder Sie verwenden können.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über bestehende SMB-Sitzungen anzuzeigen.
- Sie können den `-fields` Parameter oder den `-instance` Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Für alle Sitzungen auf der SVM in zusammengefasster Form	`vserver cifs session show -vserver vserver_name`
Bei einer bestimmten Verbindungs-ID	`vserver cifs session show -vserver vserver_name -connection-id integer`

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Von einer bestimmten Workstation IP-Adresse	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
An einer bestimmten LIF-IP-Adresse	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Auf einem bestimmten Knoten	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Von einem bestimmten Windows-Benutzer
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Mit einem festgelegten Authentifizierungsmechanismus
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Mit einer bestimmten Protokollversion	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Der permanent verfügbare Schutz und SMB Multichannel sind nur für SMB 3.0 und höhere Sitzungen verfügbar. Um deren Status für alle qualifizierenden Sitzungen anzuzeigen, sollte dieser Parameter mit dem Wert `SMB3` oder höher angegeben werden. ====
Mit einem festgelegten Niveau an kontinuierlich verfügbarem Schutz	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Wenn der Status „Dauerhaft verfügbar“ `Partial` ist, bedeutet dies, dass die Sitzung mindestens eine geöffnete, dauerhaft verfügbare Datei enthält, aber auch einige Dateien, die nicht mit dauerhaft verfügbarer Schutz geöffnet sind. Der `vserver cifs sessions file show` Befehl kann verwendet werden, um zu bestimmen, welche Dateien in der bestehenden Sitzung nicht mit dauerhaft verfügbarer Schutz geöffnet sind. ====

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Mit einem festgelegten SMB-Signing-Sitzungsstatus	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Beispiele

Der folgende Befehl zeigt Sitzungsinformationen für die Sitzungen auf SVM vs1 an, die von einer Workstation mit der IP-Adresse 10.1.1.1 aufgebaut wurden:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281 1       10.1.1.1         DOMAIN\joe          2          23s
```

Der folgende Befehl zeigt detaillierte Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz auf SVM vs1 an. Die Verbindung wurde mit dem Domänenkonto hergestellt.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
```

```
        SMB Encryption Status: Unencrypted
```

Der folgende Befehl zeigt Sitzungsinformationen zu einer Sitzung an, die SMB 3.0 und SMB Multichannel auf SVM vs1 verwendet. Im Beispiel hat sich der Benutzer von einem SMB 3.0-fähigen Client über die LIF-IP-Adresse mit dieser Freigabe verbunden; daher wurde als Authentifizierungsmechanismus standardmäßig NTLMv2 verwendet. Die Verbindung muss über Kerberos-Authentifizierung hergestellt werden, um einen dauerhaft verfügbaren Schutz zu gewährleisten.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
             **Connection IDs: 3151272607,31512726078,3151272609
           Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Verwandte Informationen

Informationen zu geöffneten SMB-Dateien

Informationen zu geöffneten ONTAP SMB-Dateien

Es lassen sich Informationen zu geöffneten SMB-Dateien anzeigen, einschließlich der SMB-Verbindungs- und Sitzungs-ID, des Host-Volumes, des Freigabenamens und des Freigabepfads. Es lassen sich Informationen zum kontinuierlich verfügbaren Schutzniveau einer Datei anzeigen, was hilfreich ist, um festzustellen, ob sich eine geöffnete Datei in einem Zustand befindet, der unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Informationen über geöffnete Dateien in einer bestehenden SMB-Sitzung können angezeigt werden. Die angezeigten Informationen sind hilfreich, wenn SMB-Sitzungsinformationen für bestimmte Dateien innerhalb

einer SMB-Sitzung ermittelt werden müssen.

Wenn Sie beispielsweise eine SMB-Sitzung haben, bei der einige der geöffneten Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und andere nicht (der Wert für das `-continuously-available` Feld in `vserver cifs session show` der Befehlsausgabe ist `Partial`), lässt sich mit diesem Befehl ermitteln, welche Dateien nicht kontinuierlich verfügbar sind.

Informationen zu allen geöffneten Dateien in etablierten SMB-Sitzungen auf Storage Virtual Machines (SVMs) können in zusammengefasster Form angezeigt werden, wenn der `vserver cifs session file show` Befehl ohne optionale Parameter verwendet wird.

In vielen Fällen ist die Ausgabemenge jedoch groß. Die angezeigten Informationen lassen sich durch Angabe optionaler Parameter anpassen. Dies kann hilfreich sein, wenn Informationen nur für eine kleine Teilmenge der geöffneten Dateien angezeigt werden sollen.

- Der optionale `-fields`Parameter ermöglicht die Anzeige der Ausgabe auf den von Ihnen ausgewählten Feldern.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über geöffnete SMB-Dateien anzuzeigen.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie geöffnete SMB-Dateien anzeigen möchten…	**Führen Sie den folgenden Befehl aus…**
In zusammengefasster Form auf der SVM	`vserver cifs session file show -vserver vserver_name`
Auf einem bestimmten Knoten	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	Bei einer bestimmten Datei-ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	Bei einer bestimmten SMB-Verbindungs-ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Bei einer bestimmten SMB-Sitzungs-ID
`vserver cifs session file show -vserver vserver_name -session-id integer`	Auf dem angegebenen Hosting Aggregat
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Auf dem angegebenen Volume

Wenn Sie geöffnete SMB-Dateien anzeigen möchten…	Führen Sie den folgenden Befehl aus…
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	Auf der angegebenen SMB-Freigabe
`vserver cifs session file show -vserver vserver_name -share share_name`	Auf dem angegebenen SMB-Pfad
`vserver cifs session file show -vserver vserver_name -path path`	Mit dem festgelegten Niveau an kontinuierlich verfügbarem Schutz
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Wenn der Status „Dauerhaft verfügbar“ `No` ist, bedeutet dies, dass diese geöffneten Dateien nicht in der Lage sind, sich nach einer Übernahme und Rückgabe unterbrechungsfrei zu erholen. Sie können sich auch nicht von einer allgemeinen Aggregat-Verschiebung zwischen Partnern in einer Hochverfügbarkeitsbeziehung erholen. ====
Mit dem angegebenen wiederverbundenen Zustand	`vserver cifs session file show -vserver vserver_name -reconnected {No

Es gibt zusätzliche optionale Parameter, mit denen Sie die Ausgaberesultate verfeinern können. Weitere Informationen zu `vserver cifs session file show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiele

Das folgende Beispiel zeigt Informationen über geöffnete Dateien auf SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

Das folgende Beispiel zeigt detaillierte Informationen zu geöffneten SMB-Dateien mit der Datei-ID 82 auf SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
```

```
-instance

                    Node: node1
                 Vserver: vs1
                 File ID: 82
           Connection ID: 104617
              Session ID: 1
               File Type: Regular
               Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
              CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
              Share Mode: rw
             Range Locks: 1
Continuously Available: Yes
            Reconnected: No
```

Verwandte Informationen

Sitzungsinformationen anzeigen

Festgestellt werden kann, welche Statistiken, Objekte und Zähler auf ONTAP SMB-Servern verfügbar sind.

Bevor Sie Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken sowie zur Überwachung der Leistung erhalten können, muss bekannt sein, welche Objekte und Zähler verfügbar sind, aus denen Daten gewonnen werden können.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie feststellen möchten…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Spezifische verfügbare Objekte	`statistics catalog object show -object object_name`
Welche Zähler stehen zur Verfügung?	`statistics catalog counter show -object object_name`

   Weitere Informationen zu `statistics catalog object show`, einschließlich der verfügbaren Objekte und Zähler, finden Sie in der "ONTAP-Befehlsreferenz".

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Beispiele

Der folgende Befehl zeigt Beschreibungen ausgewählter Statistikobjekte im Zusammenhang mit dem CIFS-

und SMB-Dateizugriff im Cluster auf der Ebene der erweiterten Berechtigungen an:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Der folgende Befehl zeigt Informationen zu einigen Zählern für das `cifs` Objekt auf der erweiterten Berechtigungsebene an:

> Dieses Beispiel zeigt nicht alle verfügbaren Zähler für das `cifs` Objekt; die Ausgabe ist gekürzt.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Verwandte Informationen

- Statistiken anzeigen
- "Statistiken Katalog Zähler Objekt anzeigen"

- "Statistiken Start"

ONTAP SMB Statistiken anzeigen

Es lassen sich verschiedene Statistiken anzeigen, darunter Statistiken zu CIFS und SMB, Auditing und BranchCache-Hashes, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Bevor Sie beginnen

Sie müssen Datenbeispiele mithilfe der `statistics start` und `statistics stop` Befehle gesammelt haben, bevor Sie Informationen über Objekte anzeigen können.

Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken für…	Eingeben…
Alle Versionen von SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x und SMB 3.0	`statistics show -object smb2`
CIFS-Subsystem des Knotens	`statistics show -object nblade_cifs`
Multiprotokoll-Audit	`statistics show -object audit_ng`
BranchCache Hash-Dienst	`statistics show -object hashd`
dynamisches DNS	`statistics show -object ddns_update`

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

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

- Welche Statistiken, Objekte und Zähler auf den Servern verfügbar sind, lässt sich feststellen.
- Überwachung von SMB-signierten Sitzungsstatistiken
- Anzeige der BranchCache Statistiken
- Statistiken dienen zur Überwachung der automatischen Knotenweiterleitungsaktivität.
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- "Einrichtung der Leistungsüberwachung"

SMB-Client-basierte Dienste bereitstellen

Offline-Dateien ermöglichen das Zwischenspeichern von Dateien für die Offline-Nutzung.

Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von ONTAP SMB-Dateien für die Offline-Nutzung zu ermöglichen

ONTAP unterstützt die Microsoft-Funktion „Offline-Dateien“ oder *Client-seitiges Caching*, mit der Dateien auf dem lokalen Host für die Offline-Nutzung zwischengespeichert werden können. Benutzer können die Offline-Dateien-Funktionalität verwenden, um auch bei unterbrochener Netzwerkverbindung weiter an Dateien zu arbeiten.

Sie können festlegen, ob Windows-Benutzerdokumente und -Programme automatisch auf einer Freigabe zwischengespeichert werden oder ob die Dateien manuell zum Zwischenspeichern ausgewählt werden müssen. Die manuelle Zwischenspeicherung ist für neue Freigaben standardmäßig aktiviert. Die offline verfügbaren Dateien werden mit der lokalen Festplatte des Windows-Clients synchronisiert. Die Synchronisierung erfolgt, wenn die Netzwerkverbindung zu einer bestimmten Speichersystemfreigabe wiederhergestellt wird.

Da Offline-Dateien und -Ordner die gleichen Zugriffsrechte behalten wie die Version der auf dem CIFS-Server gespeicherten Dateien und Ordner, muss der Benutzer über ausreichende Berechtigungen für die auf dem CIFS-Server gespeicherten Dateien und Ordner verfügen, um Aktionen an den Offline-Dateien und -Ordnern ausführen zu können.

Wenn ein Benutzer und eine andere Person im Netzwerk dieselbe Datei ändern, kann der Benutzer die lokale Version der Datei im Netzwerk speichern, die andere Version behalten oder beide speichern. Wenn der Benutzer beide Versionen behält, wird eine neue Datei mit den Änderungen des lokalen Benutzers lokal gespeichert und die zwischengespeicherte Datei mit den Änderungen aus der Version der Datei überschrieben, die auf dem CIFS-Server gespeichert ist.

Offline-Dateien können für jede Freigabe einzeln über die Freigabekonfigurationseinstellungen konfiguriert werden. Beim Erstellen oder Ändern von Freigaben steht eine von vier Offline-Ordnerkonfigurationen zur Auswahl:

- Kein Caching

  Deaktiviert das Client-seitige Caching für die Freigabe. Dateien und Ordner werden nicht automatisch lokal auf Clients zwischengespeichert und Benutzer können das Zwischenspeichern von Dateien oder Ordnern auf dem lokalen System nicht auswählen.

- Manuelle Zwischenspeicherung

  Ermöglicht die manuelle Auswahl von Dateien, die im freigegebenen Verzeichnis zwischengespeichert werden sollen. Dies ist die Standardeinstellung. Standardmäßig werden keine Dateien oder Ordner auf dem lokalen Client zwischengespeichert. Benutzer können auswählen, welche Dateien und Ordner sie lokal für die Offline-Nutzung zwischenspeichern möchten.

- Automatisches Dokumenten-Caching

  Ermöglicht das automatische Zwischenspeichern von Benutzerdokumenten auf der Freigabe. Nur Dateien und Ordner, auf die zugegriffen wird, werden lokal zwischengespeichert.

- Automatisches Programm-Caching

  Ermöglicht das automatische Zwischenspeichern von Programmen und Benutzerdokumenten auf der

Freigabe. Nur Dateien, Ordner und Programme, auf die zugegriffen wird, werden lokal zwischengespeichert. Zusätzlich gestattet diese Einstellung dem Client, lokal zwischengespeicherte ausführbare Dateien auch bei bestehender Netzwerkverbindung auszuführen.

Weitere Informationen zur Konfiguration von Offline-Dateien auf Windows-Servern und -Clients bietet die Microsoft TechNet Library.

Verwandte Informationen

- Verwendung von Roaming-Profilen zur zentralen Speicherung von Benutzerprofilen auf einem CIFS-Server, der mit der SVM verbunden ist
- Informationen zur Verwendung der Ordnerumleitung zum Speichern von Daten auf Servern
- Informationen zur Verwendung von BranchCache zum Zwischenspeichern von freigegebenen Inhalten in einer Zweigstelle
- "Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informationen zu den Anforderungen für die Verwendung von Offline ONTAP SMB-Dateien

Bevor Sie die Microsoft Offline Files Funktion mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients die Funktion unterstützen.

ONTAP Versionsanforderungen

ONTAP Releases unterstützen Offline-Dateien.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machines (SVM) unterstützt ONTAP Offline-Dateien auf allen Versionen von SMB.

Windows Client Anforderungen

Der Windows Client muss die Offline-Dateien unterstützen.

Die aktuellsten Informationen darüber, welche Windows Clients die Funktion Offline-Dateien unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"mysupport.netapp.com/matrix"

Richtlinien für die Bereitstellung von Offline ONTAP SMB-Dateien

Es gibt einige wichtige Richtlinien, die beim Bereitstellen von Offline-Dateien auf Home-Verzeichnisfreigaben zu beachten sind, bei denen die `showsnapshot` Freigabeeigenschaft auf Home-Verzeichnissen gesetzt ist.

Wenn die `showsnapshot`Freigabeeigenschaft für eine Home-Verzeichnisfreigabe festgelegt ist, für die Offline-Dateien konfiguriert sind, speichern Windows-Clients alle Snapshots im `~snapshot`Ordner im Home-Verzeichnis des Benutzers zwischen.

Windows-Clients speichern alle Snapshots im Home-Verzeichnis zwischen, wenn eine oder mehrere der folgenden Bedingungen zutreffen:

- Der Benutzer stellt das Home-Verzeichnis vom Client aus offline zur Verfügung.

Der Inhalt des `~snapshot` Ordners im Home-Verzeichnis wird einbezogen und offline verfügbar gemacht.

- Der Benutzer konfiguriert die Ordnerumleitung, um einen Ordner wie `My Documents` in das Stammverzeichnis eines Home-Verzeichnisses umzuleiten, das sich auf der CIFS-Server-Freigabe befindet.

  Manche Windows-Clients stellen den umgeleiteten Ordner automatisch offline zur Verfügung. Wenn der Ordner in das Stammverzeichnis des Benutzerverzeichnisses umgeleitet wird, ist der `~snapshot` Ordner im zwischengespeicherten Offline-Inhalt enthalten.

> Offline-Dateibereitstellungen, bei denen der `~snapshot` Ordner in den Offline-Dateien enthalten ist, sollten vermieden werden. Die Snapshots im `~snapshot` Ordner enthalten alle Daten des Volumes zu dem Zeitpunkt, an dem ONTAP den Snapshot erstellt hat. Daher verbraucht das Erstellen einer Offline-Kopie des `~snapshot` Ordners erheblichen lokalen Speicherplatz auf dem Client, beansprucht Bandbreite während der Offline-Dateisynchronisierung und erhöht die Zeit, die für die Synchronisierung der Offline-Dateien benötigt wird.

ONTAP Befehle zur Konfiguration der Offline-SMB-Dateiunterstützung

Die Unterstützung für Offline-Dateien kann mithilfe der ONTAP CLI konfiguriert werden, indem eine der vier Offline-Dateieinstellungen beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern bestehender SMB-Freigaben angegeben wird. Die manuelle Unterstützung für Offline-Dateien ist die Standardeinstellung.

Über diese Aufgabe

Bei der Konfiguration der Offline-Dateiunterstützung können Sie eine der folgenden vier Offline-Dateieinstellungen auswählen:

Einstellung	Beschreibung
`none`	Verhindert, dass Windows-Clients Dateien auf dieser Freigabe zwischenspeichern.
`manual`	Ermöglicht Benutzern auf Windows-Clients, Dateien manuell zur Zwischenspeicherung auszuwählen.
`documents`	Ermöglicht Windows-Clients, Benutzerdokumente zwischenzuspeichern, die der Benutzer für den Offline-Zugriff verwendet.
`programs`	Ermöglicht Windows-Clients, Programme, die der Benutzer verwendet, für den Offline-Zugriff zwischenzuspeichern. Clients können die zwischengespeicherten Programmdateien im Offline-Modus verwenden, selbst wenn die Freigabe verfügbar ist.

Sie können nur eine Offline-Dateieinstellung auswählen. Wenn eine Offline-Dateieinstellung für eine bestehende SMB-Freigabe geändert wird, ersetzt die neue Einstellung die ursprüngliche. Andere bestehende SMB-Freigabe-Konfigurationseinstellungen und Freigabeeigenschaften werden nicht entfernt oder ersetzt. Sie bleiben wirksam, bis sie explizit entfernt oder geändert werden.

Schritte

1. Die entsprechende Maßnahme ausführen:

Wenn Sie Offline-Dateien auf … konfigurieren möchten	Geben Sie den Befehl ein…
Eine neue SMB-Freigabe	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Eine bestehende SMB-Freigabe
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Es sollte überprüft werden, ob die SMB-Freigabekonfiguration korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Der folgende Befehl erstellt eine SMB-Freigabe mit dem Namen “data1”, wobei Offline-Dateien auf `documents` eingestellt sind:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Der folgende Befehl ändert eine vorhandene SMB-Freigabe mit dem Namen “data1”, indem die Einstellung für Offline-Dateien auf `manual` geändert und Werte für die Datei- und Verzeichnismodus-Erstellungsmaske hinzugefügt werden:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Verwandte Informationen

Freigabeeigenschaften bei bestehenden Shares hinzufügen oder entfernen

Unterstützung für Offline-Dateien auf ONTAP SMB-Freigaben mithilfe der Computer Management MMC konfigurieren

Wenn Sie Benutzern erlauben möchten, Dateien lokal für die Offline-Nutzung zwischenzuspeichern, kann die Unterstützung für Offline-Dateien mithilfe der Computer Management MMC (Microsoft Management Console) konfiguriert werden.

Schritte

1. Um die MMC auf Ihrem Windows Server zu öffnen, im Windows Explorer mit der rechten Maustaste auf das Symbol für den lokalen Computer klicken und dann **Verwalten** auswählen.
2. Im linken Bereich ist **Computerverwaltung** auszuwählen.
3. **Aktion** > **Mit einem anderen Computer verbinden** auswählen.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.

4. Den Namen des CIFS-Server eingeben oder auf **Durchsuchen** klicken, um den CIFS-Server zu suchen.

   Wenn der Name des CIFS-Servers mit dem Hostnamen der Storage Virtual Machine (SVM) übereinstimmt, ist der SVM-Name einzugeben. Wenn der Name des CIFS-Servers vom SVM-Hostnamen abweicht, ist der Name des CIFS-Servers einzugeben.

5. Klicken Sie auf **OK**.
6. In der Konsolenstruktur **System Tools** > **Freigegebene Ordner** auswählen.
7. **Teilen** auswählen.
8. Im Ergebnisbereich mit der rechten Maustaste auf die Freigabe klicken.
9. **Eigenschaften** auswählen.

   Die Eigenschaften der von Ihnen ausgewählten Freigabe werden angezeigt.

10. Im Tab **Allgemein** auf **Offline-Einstellungen** klicken.

    Das Dialogfeld „Offline-Einstellungen“ wird angezeigt.

11. Die Optionen für die Offline-Verfügbarkeit werden entsprechend konfiguriert.
12. Klicken Sie auf **OK**.

Roaming-Profile dienen dazu, Benutzerprofile zentral auf einem mit der SVM verbundenen SMB-Server zu speichern.

Informationen zur zentralen Speicherung von ONTAP SMB-Benutzerprofilen mit Roaming-Profilen

ONTAP unterstützt die Speicherung von Windows-Roaming-Profilen auf einem CIFS-Server, der der Storage Virtual Machine (SVM) zugeordnet ist. Die Konfiguration von Benutzer-Roaming-Profilen bietet Vorteile für die Benutzer, wie die automatische Verfügbarkeit von Ressourcen unabhängig davon, wo sich die Benutzer anmelden. Roaming-Profile vereinfachen außerdem die Administration und Verwaltung von Benutzerprofilen.

Roaming-Benutzerprofile haben folgende Vorteile:

- Automatische Ressourcenverfügbarkeit

  Das individuelle Benutzerprofil steht automatisch zur Verfügung, sobald sich der Benutzer an einem beliebigen Computer im Netzwerk anmeldet, auf dem Windows 8, Windows 7, Windows 2000 oder Windows XP ausgeführt wird. Benutzer müssen nicht auf jedem Computer, den sie im Netzwerk verwenden, ein Profil erstellen.

- Vereinfachter Computeraustausch

  Da alle Benutzerprofilinformationen separat im Netzwerk gespeichert werden, kann ein Benutzerprofil problemlos auf einen neuen Ersatzcomputer heruntergeladen werden. Wenn sich der Benutzer zum ersten Mal am neuen Computer anmeldet, wird die Serverkopie des Benutzerprofils auf den neuen Computer kopiert.

Verwandte Informationen

- Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von Dateien für die Offline-

Nutzung zu ermöglichen

- Informationen zur Verwendung der Ordnerumleitung zum Speichern von Daten auf Servern

Informationen zu den Anforderungen für die Verwendung von Roaming ONTAP SMB-Profilen

Bevor Sie Microsofts Roaming-Profile mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients diese Funktion unterstützen.

ONTAP Versionsanforderungen

ONTAP unterstützt Roaming-Profile.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machines (SVM) unterstützt ONTAP Roaming-Profile auf allen Versionen von SMB.

Windows Client Anforderungen

Bevor ein Benutzer die Roaming-Profile verwenden kann, muss der Windows Client diese Funktion unterstützen.

Die aktuellsten Informationen darüber, welche Windows-Clients Roaming-Profile unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"NetApp Interoperabilitätsmatrix-Tool"

Roaming-ONTAP SMB-Profile über die MMC „Active Directory-Benutzer und -Computer“ konfigurieren

Wenn das Benutzerprofil automatisch verfügbar sein soll, sobald sich der Benutzer an einem beliebigen Computer im Netzwerk anmeldet, kann die Konfiguration von Roaming-Profilen über das MMC-Snap-In Active Directory Users and Computers erfolgen. Bei der Konfiguration von Roaming-Profilen auf Windows Server kann das Active Directory Administration Center verwendet werden.

Schritte

1. Auf dem Windows-Server die MMC „Active Directory Users and Computers“ (oder das Active Directory Administration Center auf Windows-Servern) öffnen.
2. Den Benutzer ermitteln, für den ein Roaming-Profil konfiguriert werden soll.
3. Mit der rechten Maustaste auf den Benutzer klicken und auf **Eigenschaften** klicken.
4. Auf der Registerkarte **Profil** den Profilpfad zu der Freigabe eingeben, in der das Roaming-Profil des Benutzers gespeichert werden soll, gefolgt von `%username%`.

   Ein Profilpfad könnte beispielsweise wie folgt aussehen: `\\vs1.example.com\profiles\%username%`. Beim ersten Anmelden eines Benutzers wird `%username%` durch den Benutzernamen ersetzt.

   > Im Pfad `\\vs1.example.com\profiles\%username%`, `profiles` ist der Freigabename einer Freigabe auf der Storage Virtual Machine (SVM) vs1, die Vollzugriffsrechte für Everyone hat.

5. Klicken Sie auf **OK**.

Die Ordnerumleitung ermöglicht das Speichern von Daten auf einem SMB-Server.

Informationen zur Verwendung der Ordnerumleitung zur Speicherung von Daten auf ONTAP SMB-Servern

ONTAP unterstützt die Microsoft Ordnerumleitung, mit der Benutzer oder Administratoren den Pfad eines lokalen Ordners auf einen Speicherort auf dem CIFS-Server umleiten können. Es erscheint so, als ob umgeleitete Ordner auf dem lokalen Windows-Client gespeichert wären, obwohl die Daten auf einer SMB-Freigabe gespeichert sind.

Die Ordnerumleitung ist hauptsächlich für Organisationen vorgesehen, die bereits Home-Verzeichnisse eingerichtet haben und die Kompatibilität mit ihrer bestehenden Home-Verzeichnisumgebung beibehalten möchten.

- `Documents`, `Desktop` und `Start Menu` sind Beispiele für Ordner, die umgeleitet werden können.
- Benutzer können Ordner von ihrem Windows-Client aus umleiten.
- Administratoren können die Ordnerumleitung zentral konfigurieren und verwalten, indem sie GPOs in Active Directory konfigurieren.
- Wenn Administratoren Roaming-Profile konfiguriert haben, ermöglicht die Ordnerumleitung Administratoren, Benutzerdaten von Profildaten zu trennen.
- Administratoren können Ordnerumleitung und Offline-Dateien zusammen verwenden, um die Datenspeicherung für lokale Ordner auf den CIFS-Server umzuleiten, während Benutzern ermöglicht wird, die Inhalte lokal zwischenzuspeichern.

Verwandte Informationen

- Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von Dateien für die Offline-Nutzung zu ermöglichen
- Verwendung von Roaming-Profilen zur zentralen Speicherung von Benutzerprofilen auf einem CIFS-Server, der mit der SVM verbunden ist

Informationen zu den Voraussetzungen für die Verwendung der ONTAP SMB-Ordnerumleitung

Bevor Sie die Ordnerumleitung von Microsoft mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients diese Funktion unterstützen.

ONTAP Versionsanforderungen

ONTAP unterstützt die Umleitung von Microsoft Ordnern.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machine (SVM) unterstützt ONTAP die Ordnerumleitung von Microsoft in allen Versionen von SMB.

Windows Client Anforderungen

Bevor ein Benutzer die Ordnerumleitung von Microsoft verwenden kann, muss der Windows Client diese

Funktion unterstützen.

Die aktuellsten Informationen darüber, welche Windows-Clients die Ordnerumleitung unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"mysupport.netapp.com/matrix"

ONTAP SMB-Ordnerumleitung mithilfe der Windows-Eigenschaften konfigurieren

Die Ordnerumleitung kann über das Windows-Eigenschaftenfenster konfiguriert werden. Der Vorteil dieser Methode besteht darin, dass der Windows-Benutzer die Ordnerumleitung ohne Unterstützung des SVM-Administrators konfigurieren kann.

Schritte

1. Im Windows Explorer mit der rechten Maustaste auf den Ordner klicken, der auf eine Netzwerkfreigabe umgeleitet werden soll.
2. **Eigenschaften** auswählen.

   Die Eigenschaften der von Ihnen ausgewählten Freigabe werden angezeigt.

3. Im Tab **Verknüpfung** auf **Ziel** klicken und den Pfad zum Netzwerkstandort angeben, zu dem der ausgewählte Ordner umgeleitet werden soll.

   Wenn beispielsweise ein Ordner in den `data` Ordner in einem Home-Verzeichnis umgeleitet werden soll, das auf `Q:\` zugeordnet ist, ist `Q:\data` als Ziel anzugeben.

4. Klicken Sie auf **OK**.

   Weitere Informationen zur Konfiguration von Offline-Ordnern bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informationen zum Zugriff auf das ONTAP ~snapshot-Verzeichnis von Windows-Clients mit SMB 2.x

Die Methode, mit der Sie von Windows-Clients mithilfe von SMB 2.x auf das `~snapshot` Verzeichnis zugreifen, unterscheidet sich von der Methode, die für SMB 1.0 verwendet wird. Es ist erforderlich zu verstehen, wie auf das `~snapshot` Verzeichnis bei der Nutzung von SMB 2.x-Verbindungen zugegriffen werden kann, um erfolgreich auf in Snapshots gespeicherte Daten zuzugreifen.

Der SVM-Administrator steuert, ob Benutzer auf Windows-Clients das `~snapshot` Verzeichnis auf einer Freigabe anzeigen und darauf zugreifen können, indem die `showsnapshot` Freigabeeigenschaft mithilfe von Befehlen aus den vserver cifs share properties-Familien aktiviert oder deaktiviert wird.

Wenn die `showsnapshot` Freigabeeigenschaft deaktiviert ist, kann ein Benutzer auf einem Windows-Client, der SMB 2.x verwendet, das `~snapshot` Verzeichnis nicht anzeigen und nicht auf Snapshots innerhalb des `~snapshot` Verzeichnisses zugreifen, selbst wenn der Pfad zum `~snapshot` Verzeichnis oder zu bestimmten Snapshots innerhalb des Verzeichnisses manuell eingegeben wird.

Wenn die `showsnapshot`Freigabeeigenschaft aktiviert ist, kann ein Benutzer auf einem Windows-Client, der SMB 2.x verwendet, das `~snapshot`Verzeichnis weder im Stammverzeichnis der Freigabe noch in einer Verbindung oder einem Verzeichnis unterhalb des Stammverzeichnisses der Freigabe anzeigen. Nach dem Verbindungsaufbau zu einer Freigabe kann der Benutzer jedoch auf das versteckte `~snapshot`Verzeichnis zugreifen, indem `\~snapshot`manuell an das Ende des Freigabepfads angehängt wird. Das versteckte `~snapshot`Verzeichnis ist über zwei Einstiegspunkte erreichbar:

- Im Stammverzeichnis der Freigabe
- An jedem Verbindungspunkt im Share Space

Das versteckte `~snapshot`Verzeichnis ist von nicht-Verbindungs-Unterverzeichnissen innerhalb der Freigabe nicht zugänglich.

Beispiel

Mit der im folgenden Beispiel gezeigten Konfiguration kann ein Benutzer auf einem Windows-Client mit einer SMB 2.x-Verbindung zur Freigabe „eng“ auf das `~snapshot`Verzeichnis zugreifen, indem `\~snapshot`zum Freigabepfad am Stamm der Freigabe und an jedem Verbindungspunkt im Pfad manuell hinzugefügt wird. Das versteckte `~snapshot`Verzeichnis ist über die folgenden drei Pfade zugänglich:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ---------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Dateien und Ordner mit vorherigen Versionen wiederherstellen

Informationen zur Wiederherstellung von ONTAP SMB-Dateien und -Ordnern mit früheren Versionen

Die Möglichkeit, Microsoft Previous Versions zu nutzen, ist für Dateisysteme verfügbar, die Snapshots in irgendeiner Form unterstützen und diese aktiviert haben. Snapshot Technologie ist ein integraler Bestandteil von ONTAP. Benutzer können Dateien und Ordner aus Snapshots von ihrem Windows-Client mithilfe der Funktion Microsoft

Previous Versions wiederherstellen.

Die Funktion „Vorherige Versionen“ bietet eine Methode für Benutzer, Snapshots zu durchsuchen oder Daten aus einem Snapshot wiederherzustellen, ohne dass ein Speicheradministrator eingreifen muss. „Vorherige Versionen“ ist nicht konfigurierbar. Sie ist immer aktiviert. Wenn der Speicheradministrator Snapshots auf einer Freigabe bereitgestellt hat, kann der Benutzer mit „Vorherige Versionen“ die folgenden Aufgaben ausführen:

- Wiederherstellung versehentlich gelöschter Dateien.
- Wiederherstellung nach versehentlichem Überschreiben einer Datei.
- Dateiversionen während der Bearbeitung vergleichen.

Die in Snapshots gespeicherten Daten sind schreibgeschützt. Benutzer müssen eine Kopie einer Datei an einem anderen Speicherort speichern, um Änderungen an der Datei vorzunehmen. Snapshots werden regelmäßig gelöscht, daher müssen Benutzer Kopien der in „Vorherige Versionen“ enthaltenen Dateien erstellen, wenn sie eine frühere Version einer Datei dauerhaft aufbewahren möchten.

ONTAP SMB-Anforderungen für die Verwendung von Microsoft Previous Versions

Bevor Sie „Vorherige Versionen“ mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients dies unterstützen. Sie müssen außerdem die Anforderung an die Snapshot-Einstellung kennen.

ONTAP Versionsanforderungen

Unterstützt frühere Versionen.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machines (SVM) unterstützt ONTAP Previous Versions auf allen Versionen von SMB.

Windows Client Anforderungen

Bevor ein Benutzer mit der Funktion „Vorherige Versionen“ auf Daten in Snapshots zugreifen kann, muss der Windows Client diese Funktion unterstützen.

Die aktuellsten Informationen darüber, welche Windows Clients Previous Versions unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"NetApp Interoperabilitätsmatrix-Tool"

Anforderungen an Snapshot-Einstellungen

Um mit Hilfe von „Vorherige Versionen“ auf Daten in Snapshots zugreifen zu können, muss dem Volume, das die Daten enthält, eine aktivierte Snapshot-Richtlinie zugeordnet sein, Clients müssen auf die Snapshot-Daten zugreifen können und Snapshots müssen vorhanden sein.

ONTAP SMB-Snapshot-Daten lassen sich mit der Registerkarte „Windows Vorherige Versionen“ anzeigen und verwalten.

Benutzer auf Windows-Clientrechnern können die Registerkarte „Vorherige Versionen“ im Fenster „Windows-Eigenschaften“ verwenden, um Daten wiederherzustellen, die in

Snapshots gespeichert sind, ohne den Administrator der Storage Virtual Machine (SVM) einbeziehen zu müssen.

Über diese Aufgabe

Die Registerkarte „Vorherige Versionen“ kann nur zum Anzeigen und Verwalten von Daten in Snapshots von auf der SVM gespeicherten Daten verwendet werden, wenn der Administrator Snapshots auf dem Volume, das die Freigabe enthält, aktiviert hat und die Freigabe so konfiguriert ist, dass Snapshots angezeigt werden.

Schritte

1. Im Windows Explorer werden die Inhalte des zugeordneten Laufwerks mit den auf dem CIFS-Server gespeicherten Daten angezeigt.
2. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner im zugeordneten Netzlaufwerk, dessen Snapshots Sie anzeigen oder verwalten möchten.
3. **Eigenschaften** auswählen.

   Die Eigenschaften der ausgewählten Datei oder des ausgewählten Ordners werden angezeigt.

4. Die Registerkarte **Vorherige Versionen** auswählen.

   Im Feld „Ordnerversionen“ wird eine Liste der verfügbaren Snapshots der ausgewählten Datei oder des ausgewählten Ordners angezeigt. Die aufgelisteten Snapshots werden durch das Snapshot-Namenspräfix und den Erstellungszeitstempel identifiziert.

5. Im Feld **Ordnerversionen:** mit der rechten Maustaste auf die Kopie der Datei oder des Ordners klicken, die verwaltet werden soll.
6. Die entsprechende Maßnahme ausführen:

Wenn Sie möchten…	Führen Sie folgende Schritte aus…
Daten aus diesem Snapshot anzeigen	Auf **Öffnen** klicken.
Eine Kopie der Daten aus diesem Snapshot erstellen	Auf **Kopieren** klicken.

   Die Daten in Snapshots sind schreibgeschützt. Wenn Änderungen an den im Tab „Vorherige Versionen“ aufgeführten Dateien und Ordnern vorgenommen werden sollen, ist eine Kopie der zu ändernden Dateien und Ordner an einem beschreibbaren Speicherort zu speichern und die Änderungen an den Kopien vorzunehmen.

7. Nachdem Sie die Verwaltung der Snapshot-Daten abgeschlossen haben, wird das Dialogfeld **Eigenschaften** durch Klicken auf **OK** geschlossen.

   Weitere Informationen zur Verwendung der Registerkarte „Vorherige Versionen“ zum Anzeigen und Verwalten von Snapshot-Daten bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Es kann festgestellt werden, ob ONTAP SMB Snapshots für die Verwendung mit Previous Versions verfügbar sind.

Snapshots können auf der Registerkarte „Vorherige Versionen“ nur angezeigt werden, wenn für das Volume, das die Freigabe enthält, eine aktivierte Snapshot-Richtlinie gilt

und die Volume-Konfiguration den Zugriff auf Snapshots zulässt. Die Ermittlung der Snapshot-Verfügbarkeit ist hilfreich, wenn einem Benutzer beim Zugriff auf frühere Versionen Unterstützung geboten wird.

Schritte

1. Es wird geprüft, ob für das Volume, auf dem sich die Freigabedaten befinden, automatische Snapshots aktiviert sind und ob Clients Zugriff auf die Snapshot-Verzeichnisse haben: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   Die Ausgabe zeigt an, welche Snapshot-Richtlinie dem Volume zugeordnet ist, ob der Zugriff auf das Client-Snapshot-Verzeichnis aktiviert ist und wie viele Snapshots verfügbar sind.

2. Es wird geprüft, ob die zugehörige Snapshot-Richtlinie aktiviert ist: `volume snapshot policy show -policy policy-name`
3. Liste der verfügbaren Snapshots: `volume snapshot show -volume volume_name`

   Weitere Informationen zum Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen sind unter "Datensicherung" zu finden.

Beispiel

Das folgende Beispiel zeigt Informationen zu den Snapshot-Richtlinien, die dem Volume mit dem Namen “data1” zugeordnet sind, das die gemeinsam genutzten Daten und die verfügbaren Snapshots auf “data1” enthält.

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                  ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------ -------- -------- ------ -----
```

```
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Verwandte Informationen

- Snapshot-Konfigurationen erstellen, um den Zugriff auf frühere Versionen zu ermöglichen
- "Datenschutz"

ONTAP SMB Snapshot-Konfigurationen erstellen, um den Zugriff auf frühere Versionen zu ermöglichen

Die Funktion „Vorherige Versionen“ ist immer verfügbar, sofern der Clientzugriff auf Snapshots aktiviert ist und Snapshots vorhanden sind. Wenn Ihre Snapshot-Konfiguration diese Anforderungen nicht erfüllt, kann eine Snapshot-Konfiguration erstellt werden, die diese Anforderungen erfüllt.

Schritte

1. Wenn dem Volume, das die Freigabe enthält, für die Sie den Zugriff auf frühere Versionen zulassen möchten, keine Snapshot-Richtlinie zugeordnet ist, muss dem Volume eine Snapshot-Richtlinie zugeordnet und diese mit dem `volume modify` Befehl aktiviert werden.

   Weitere Informationen zu `volume modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Der Zugriff auf die Snapshots wird ermöglicht, indem der `volume modify` Befehl verwendet wird, um die `-snap-dir` Option auf `true` zu setzen.

   Weitere Informationen zu `volume modify` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, ob die Snapshot-Richtlinien aktiviert sind und der Zugriff auf die Snapshot-Verzeichnisse aktiviert ist, indem die `volume show`- und `volume snapshot policy show`-Befehle verwendet werden.

   Weitere Informationen zu `volume show` und `volume snapshot policy show` finden sich in der "ONTAP-Befehlsreferenz".

   Weitere Informationen zum Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen sind unter "Datensicherung" zu finden.

Verwandte Informationen

"Datenschutz"

Informationen zur Wiederherstellung von Verzeichnissen mit früheren Versionen, die ONTAP SMB-Verbindungen enthalten

Bestimmte Richtlinien sind zu beachten, wenn „Vorherige Versionen“ zum Wiederherstellen von Ordnern mit Verbindungspunkten verwendet wird.

Wenn „Vorherige Versionen“ zum Wiederherstellen von Ordnern verwendet wird, die untergeordnete Ordner als Verbindungspunkte enthalten, kann die Wiederherstellung mit einem `Access Denied` Fehler fehlschlagen.

Es lässt sich feststellen, ob der Ordner, den Sie wiederherstellen möchten, eine Verbindung enthält, indem der `vol show` Befehl mit der `-parent` Option verwendet wird. Auch die `vserver security trace` Befehle können genutzt werden, um detaillierte Protokollierung zu Problemen beim Dateizugriff und Ordnerzugriff zu erstellen.

Verwandte Informationen

Erstellen und Verwalten von Datenvolumes in NAS-Namespaces

Bereitstellung von SMB serverbasierten Diensten

Home-Verzeichnisse verwalten

Informationen zur Aktivierung dynamischer Home Directorys auf ONTAP SMB-Servern

ONTAP Home Directorys ermöglichen die Konfiguration einer SMB-Freigabe, die je nach Benutzer, der sich verbindet, und einer Reihe von Variablen unterschiedlichen Verzeichnissen zugeordnet wird. Anstatt für jeden Benutzer separate Freigaben zu erstellen, kann eine einzige Freigabe mit wenigen Home Directory-Parametern konfiguriert werden, um die Beziehung eines Benutzers zwischen einem Einstiegspunkt (der Freigabe) und dem Home Directory (einem Verzeichnis auf der SVM) zu definieren.

Ein als Gastbenutzer angemeldeter Benutzer besitzt kein Home Directory und kann nicht auf die Home Directories anderer Benutzer zugreifen. Es gibt vier Variablen, die bestimmen, wie ein Benutzer einem Verzeichnis zugeordnet wird:

- **Freigabename**

  Dies ist der Name der Freigabe, die Sie erstellen, mit der sich der Benutzer verbindet. Für diese Freigabe muss die Home Directory-Eigenschaft festgelegt werden.

  Der Freigabename kann die folgenden dynamischen Namen verwenden:

  - `%w` (der Windows-Benutzername des Benutzers)
  - `%d` (der Windows-Domänenname des Benutzers)
  - `%u` (der zugeordnete UNIX-Benutzername des Benutzers) Um den Freigabenamen in allen Home-Verzeichnissen eindeutig zu machen, muss der Freigabename entweder die /`%w` oder die `%u` Variable enthalten. Der Freigabename kann sowohl die `%d` als auch die /`%w` Variable enthalten (zum Beispiel `%d` /`%w`), oder der Freigabename kann einen statischen und einen variablen Teil enthalten (zum Beispiel home_/`%w`).
- **Freigabepfad**

Dies ist der relative Pfad, der durch die Freigabe definiert und daher einem der Freigabenamen zugeordnet ist, der an jeden Suchpfad angehängt wird, um den vollständigen Home Directory-Pfad des Benutzers vom Stammverzeichnis der SVM aus zu generieren. Er kann statisch sein (zum Beispiel, `home`), dynamisch sein (zum Beispiel, `%w`), oder eine Kombination aus beidem (zum Beispiel, `eng/%w`).

- **Suchpfade**

  Dies ist die Menge absoluter Pfade vom Stammverzeichnis der SVM, die Sie angeben und die die ONTAP-Suche nach Home Directorys steuern. Es können ein oder mehrere Suchpfade mit dem `vserver cifs home-directory search-path add` Befehl angegeben werden. Wenn mehrere Suchpfade angegeben werden, versucht ONTAP diese in der angegebenen Reihenfolge, bis ein gültiger Pfad gefunden wird. Weitere Informationen zu `vserver cifs home-directory search-path add` finden sich in der "ONTAP-Befehlsreferenz".

- **Verzeichnis**

  Dies ist das Home Directory des Benutzers, das für den Benutzer erstellt wird. Der Verzeichnisname ist üblicherweise der Name des Benutzers. Das Home Directory muss in einem der Verzeichnisse erstellt werden, die durch die Suchpfade definiert sind.

Als Beispiel kann folgendes Setup betrachtet werden:

- Benutzer: John Smith
- Benutzerdomäne: acme
- Benutzername: jsmith
- SVM-Name: vs1
- Home-Verzeichnis-Freigabename #1: home_ `%w` - Freigabepfad: `%w`
- Home-Verzeichnis-Freigabename #2: `%w` - Freigabepfad: `%d/%w`
- Suchpfad Nr. 1: `/vol0home/home`
- Suchpfad Nr. 2: `/vol1home/home`
- Suchpfad Nr. 3: `/vol2home/home`
- Home-Verzeichnis: `/vol1home/home/jsmith`

Szenario 1: Der Benutzer stellt eine Verbindung zu `\\vs1\home_jsmith` her. Dies entspricht dem Namen der ersten Home-Verzeichnisfreigabe und generiert den relativen Pfad `jsmith`. ONTAP sucht nun nach einem Verzeichnis mit dem Namen `jsmith`, indem jeder Suchpfad der Reihe nach überprüft wird:

- `/vol0home/home/jsmith`Existiert nicht, es wird mit Suchpfad Nr. 2 fortgefahren.
- `/vol1home/home/jsmith`existiert; daher wird Suchpfad Nr. 3 nicht überprüft; der Benutzer ist nun mit seinem Home-Verzeichnis verbunden.

Szenario 2: Der Benutzer stellt eine Verbindung zu `\\vs1\jsmith` her. Dies entspricht dem Namen der zweiten Home-Verzeichnisfreigabe und generiert den relativen Pfad `acme/jsmith`. ONTAP sucht nun nach einem Verzeichnis mit dem Namen `acme/jsmith`, indem jeder Suchpfad der Reihe nach überprüft wird:

- `/vol0home/home/acme/jsmith`Existiert nicht, es wird mit Suchpfad Nr. 2 fortgefahren.
- `/vol1home/home/acme/jsmith`Existiert nicht, es wird mit Suchpfad Nr. 3 fortgefahren.
- `/vol2home/home/acme/jsmith` existiert nicht; das Home-Verzeichnis existiert nicht; daher schlägt die

Verbindung fehl.

ONTAP SMB-Homeverzeichnisfreigaben hinzufügen

Wenn Sie die SMB Home-Verzeichnisfunktion nutzen möchten, muss mindestens eine Freigabe mit der Home-Verzeichnis-Eigenschaft in den Freigabeeigenschaften hinzugefügt werden.

Über diese Aufgabe

Sie können eine Home-Verzeichnisfreigabe zum Zeitpunkt der Erstellung der Freigabe mit dem `vserver cifs share create` Befehl erstellen, oder eine bestehende Freigabe jederzeit mit dem `vserver cifs share modify` Befehl in eine Home-Verzeichnisfreigabe umwandeln.

Um eine Home-Verzeichnisfreigabe zu erstellen, muss der Wert `homedirectory` in der Option `-share -properties` beim Erstellen oder Ändern einer Freigabe angegeben werden. Der Freigabename und der Freigabepfad können mithilfe von Variablen festgelegt werden, die beim Verbinden der Benutzer mit ihren Home-Verzeichnissen dynamisch erweitert werden. Verfügbare Variablen, die im Pfad verwendet werden können, sind `%w`, `%d` und `%u`, die jeweils dem Windows-Benutzernamen, der Domäne und dem zugeordneten UNIX-Benutzernamen entsprechen.

Schritte

1. Eine Home-Verzeichnisfreigabe hinzufügen:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver` `vserver`Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

   `-share-name` *`share-name`* gibt den Namen der Home-Verzeichnisfreigabe an.

   Zusätzlich zur Angabe einer der erforderlichen Variablen muss, falls der Freigabename eine der Literalzeichenfolgen `%w`, `%u` oder `%d` enthält, der Literalzeichenfolge ein % (Prozent) Zeichen vorangestellt werden, um zu verhindern, dass ONTAP die Literalzeichenfolge als Variable behandelt (zum Beispiel `%%w`).

   - Der Freigabename muss entweder die `%w`- oder die `%u`-Variable enthalten.
   - Der Freigabename kann zusätzlich die `%d` Variable (zum Beispiel `%d`/`%w`) oder einen statischen Teil im Freigabenamen (zum Beispiel home1_/`%w`) enthalten.
   - Wenn die Freigabe von Administratoren verwendet wird, um eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen oder um Benutzern zu erlauben, eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen, muss dem dynamischen Freigabenamensmuster eine Tilde (~) vorangestellt werden.

     Das `vserver cifs home-directory modify` wird verwendet, um diesen Zugriff zu ermöglichen, indem die `-is-home-dirs-access-for-admin-enabled` Option auf `true` gesetzt wird oder indem die erweiterte Option `-is-home-dirs-access-for-public-enabled` auf `true` gesetzt wird.

   `-path path` Gibt den relativen Pfad zum Home Directory an.

`-share-properties homedirectory[,…]` Gibt die Eigenschaften dieser Freigabe an. Der `homedirectory` Wert muss angegeben werden. Zusätzliche Freigabeeigenschaften können mit einer durch Kommas getrennten Liste angegeben werden.

1. Es kann mit dem `vserver cifs share show` Befehl überprüft werden, ob die Freigabe des Home-Verzeichnisses erfolgreich hinzugefügt wurde.

Beispiel

Der folgende Befehl erstellt eine Home-Verzeichnisfreigabe mit dem Namen `%w`. Die `oplocks`, `browsable` und `changenotify` Freigabeeigenschaften werden zusätzlich zur Einstellung der `homedirectory` Freigabeeigenschaft festgelegt.

> Dieses Beispiel zeigt nicht die Ausgabe für alle Shares auf der SVM an. Die Ausgabe ist gekürzt.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Verwandte Informationen

- Suchpfade für das Home-Verzeichnis hinzufügen
- Anforderungen und Richtlinien für die Verwendung automatischer Knotenverweise auf Servern
- Zugänglichkeit zu Benutzer-Home-Verzeichnissen verwalten

Informationen zu den einzigartigen ONTAP SMB-Benutzernamenanforderungen für Home-Verzeichnis-Freigaben

Achten Sie darauf, beim Erstellen von Home-Verzeichnisfreigaben mithilfe der `%w` (Windows-Benutzername) oder `%u` (UNIX-Benutzername) Variablen zur dynamischen Generierung von Freigaben eindeutige Benutzernamen zu vergeben. Der Freigabename wird Ihrem Benutzernamen zugeordnet.

Zwei Probleme können auftreten, wenn der Name einer statischen Freigabe und der Benutzername identisch sind:

- Wenn der Benutzer die Freigaben in einem Cluster mit dem `net view` Befehl auflistet, werden zwei Freigaben mit dem gleichen Benutzernamen angezeigt.
- Wenn sich der Benutzer mit diesem Freigabenamen verbindet, wird er immer mit der statischen Freigabe verbunden und kann nicht auf die Home-Verzeichnis-Freigabe mit demselben Namen zugreifen.

Beispielsweise gibt es eine Freigabe mit dem Namen „administrator“ und Sie haben einen Windows-Benutzernamen „administrator“. Wenn eine Home-Verzeichnis-Freigabe erstellt und eine Verbindung zu dieser Freigabe hergestellt wird, erfolgt die Verbindung mit der statischen Freigabe „administrator“, nicht mit der

Home-Verzeichnis-Freigabe „administrator“.

Das Problem mit doppelten Freigabenamen kann durch einen der folgenden Schritte behoben werden:

- Die statische Freigabe wird umbenannt, sodass sie nicht mehr mit der Freigabe des Home-Verzeichnisses des Benutzers in Konflikt steht.
- Dem Benutzer einen neuen Benutzernamen zuweisen, damit dieser nicht mehr mit dem statischen Freigabenamen in Konflikt steht.
- Erstellen einer CIFS-Home-Verzeichnisfreigabe mit einem statischen Namen wie “home”, anstatt den `%w` Parameter zu verwenden, um Konflikte mit den Freigabenamen zu vermeiden.

Informationen darüber, was mit statischen ONTAP SMB-Homeverzeichnis-Freigabenamen nach einem Upgrade geschieht

Die Namen von Home-Verzeichnisfreigaben müssen entweder die `%w` oder die `%u` dynamische Variable enthalten. Es ist zu beachten, was mit bestehenden statischen Home-Verzeichnisfreigabenamen nach einem Upgrade auf eine Version von ONTAP mit dieser neuen Anforderung geschieht.

Wenn Ihre Home-Verzeichniskonfiguration statische Freigabenamen enthält und Sie auf ONTAP aktualisieren, bleiben die statischen Home-Verzeichnisfreigabenamen unverändert und weiterhin gültig. Es können jedoch keine neuen Home-Verzeichnisfreigaben erstellt werden, die nicht entweder die `%w` oder `%u` Variable enthalten.

Die Anforderung, dass eine dieser Variablen im Freigabenamen des Benutzerverzeichnisses enthalten ist, gewährleistet, dass jeder Freigabename innerhalb der Benutzerverzeichniskonfiguration eindeutig ist. Falls gewünscht, können die statischen Freigabenamen des Benutzerverzeichnisses in Namen geändert werden, die entweder die `%w` oder die `%u` Variable enthalten.

ONTAP SMB Home-Verzeichnis-Suchpfade hinzufügen

Wenn Sie ONTAP SMB Home-Verzeichnisse verwenden möchten, muss mindestens ein Suchpfad für das Home-Verzeichnis hinzugefügt werden.

Über diese Aufgabe

Ein Suchpfad für das Home-Verzeichnis kann mit dem `vserver cifs home-directory search-path add` Befehl hinzugefügt werden.

Der `vserver cifs home-directory search-path add` Befehl prüft den im `-path` angegebenen Pfad während der Befehlsausführung. Wenn der angegebene Pfad nicht existiert, erzeugt der Befehl eine Meldung mit der Aufforderung, ob fortgefahren werden soll. Es kann `y` oder `n` ausgewählt werden. Wenn `y` das Fortfahren gewählt wird, erstellt ONTAP den Suchpfad. Die Verzeichnisstruktur muss jedoch erstellt werden, bevor der Suchpfad in der Home Directory Konfiguration verwendet werden kann. Wenn das Fortfahren nicht gewählt wird, schlägt der Befehl fehl, der Suchpfad wird nicht erstellt. Anschließend kann die Verzeichnisstruktur für den Pfad erstellt und der `vserver cifs home-directory search-path add` Befehl erneut ausgeführt werden.

Schritte

1. Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Es wird überprüft, ob der Suchpfad erfolgreich mit dem `vserver cifs home-directory search-`

`path show` Befehl hinzugefügt wurde.

Beispiel

Das folgende Beispiel fügt den Pfad `/home1` zur Home-Verzeichnis-Konfiguration auf SVM vs1 zur Home-Verzeichnis-Konfiguration hinzu.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Im folgenden Beispiel wird versucht, den Pfad `/home2` zur Home-Verzeichniskonfiguration auf SVM vs1 hinzuzufügen. Der Pfad existiert nicht. Es wird entschieden, nicht fortzufahren.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Verwandte Informationen

Freigaben des Home-Verzeichnisses hinzufügen

ONTAP SMB Home Directory-Konfigurationen mit den Variablen %w und %d erstellen

Es ist möglich, eine Home Directory-Konfiguration mit den Variablen `%w` und `%d` zu erstellen. Anwender können sich anschließend über dynamisch erstellte Freigaben mit ihrem Home-Share verbinden.

Schritte

1. Einen Qtree erstellen, der die Home Directory-Pfade der Benutzer enthält: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Es sollte überprüft werden, ob der Qtree den korrekten Sicherheitsstil verwendet: `volume qtree show`
3. Falls der Qtree nicht den gewünschten Sicherheitsstil verwendet, kann der Sicherheitsstil mit dem `volume qtree security` Befehl geändert werden.
4. Eine Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver` `vserver`Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

   `-share-name` `%w` Gibt den Namen der Home Directory-Freigabe an. ONTAP erstellt den Freigabenamen

dynamisch, wenn sich ein Benutzer mit seinem Home Directory verbindet. Der Freigabename hat die Form *windows_user_name*.

`-path %d/%w` Gibt den relativen Pfad zum Home Directory an. Der relative Pfad wird dynamisch erstellt, wenn sich ein Benutzer mit seinem Home Directory verbindet, und hat die Form *domain/windows_user_name*.

`-share-properties homedirectory[,…]+` Gibt die Eigenschaften dieser Freigabe an. Der `homedirectory` Wert muss angegeben werden. Zusätzliche Freigabeeigenschaften können mit einer durch Kommas getrennten Liste angegeben werden.

5. Es kann überprüft werden, ob die Freigabe die gewünschte Konfiguration aufweist, indem der `vserver cifs share show` Befehl verwendet wird.
6. Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver *vserver-name*`Gibt die CIFS-fähige SVM an, zu der der Suchpfad hinzugefügt wird.

   `-path *path*`gibt den absoluten Verzeichnispfad zum Suchpfad an.

7. Es wird überprüft, ob der Suchpfad erfolgreich mit dem `vserver cifs home-directory search-path show` Befehl hinzugefügt wurde.
8. Für Benutzer mit einem Home Directory wird ein entsprechendes Verzeichnis im Qtree oder Volume erstellt, das für die Aufnahme von Home Directories vorgesehen ist.

   Wenn beispielsweise ein Qtree mit dem Pfad `/vol/vol1/users` und dem Benutzernamen, dessen Verzeichnis erstellt werden soll, mydomain\user1 vorhanden ist, wird ein Verzeichnis mit dem folgenden Pfad erstellt: `/vol/vol1/users/mydomain/user1`.

   Wenn ein Volume mit dem Namen “home1” erstellt und unter `/home1` gemountet wurde, würde ein Verzeichnis mit folgendem Pfad erstellt: `/home1/mydomain/user1`.

9. Es wird überprüft, ob ein Benutzer erfolgreich eine Verbindung zum Home Share herstellen kann, entweder durch das Zuordnen eines Laufwerks oder durch das Verbinden über den UNC-Pfad.

   Wenn beispielsweise der Benutzer mydomain\user1 eine Verbindung zu dem in Schritt 8 erstellten Verzeichnis herstellen möchte, das sich auf SVM vs1 befindet, würde user1 die Verbindung über den UNC-Pfad `\\vs1\user1` herstellen.

Beispiel

Die Befehle im folgenden Beispiel erstellen eine Home Directory-Konfiguration mit den folgenden Einstellungen:

- Der Freigabename ist %w.
- Der relative Home Directory-Pfad ist %d/%w.
- Der Suchpfad, der die Home-Verzeichnisse enthält, `/home1`, ist ein Volume, das mit dem NTFS-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM vs1 erstellt.

Diese Art der Home-Verzeichnis-Konfiguration kann verwendet werden, wenn Benutzer von Windows-Hosts auf ihre Home-Verzeichnisse zugreifen. Diese Konfiguration kann ebenfalls verwendet werden, wenn Benutzer

sowohl von Windows- als auch von UNIX-Hosts auf ihre Home-Verzeichnisse zugreifen und der Systemadministrator Windows-basierte Benutzer und Gruppen zur Steuerung des Zugriffs auf das Dateisystem verwendet.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Verwandte Informationen

- Home-Verzeichnisse mit der Variablen %u konfigurieren
- Zusätzliche Home Directory-Konfigurationen werden erläutert.
- Informationen zu Home Directory-Pfaden von Benutzern anzeigen

ONTAP SMB-Home-Verzeichnisse mit der Variablen %u konfigurieren

Sie können eine Home Directory-Konfiguration erstellen, bei der der Freigabename mit der `%w` Variable festgelegt wird, während die `%u` Variable verwendet wird, um den relativen Pfad zur Home Directory-Freigabe anzugeben. Benutzer können sich dann mit

ihrer Home Directory-Freigabe verbinden, indem sie dynamisch erstellte Freigaben mit ihrem Windows-Benutzernamen verwenden, ohne den tatsächlichen Namen oder Pfad des Home Directory zu kennen.

Schritte

1. Einen Qtree erstellen, der die Home Directory-Pfade der Benutzer enthält: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Es sollte überprüft werden, ob der Qtree den korrekten Sicherheitsstil verwendet: `volume qtree show`
3. Falls der Qtree nicht den gewünschten Sicherheitsstil verwendet, kann der Sicherheitsstil mit dem `volume qtree security` Befehl geändert werden.
4. Eine Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver` `vserver`Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

   `-share-name %w` Gibt den Namen der Home Directory-Freigabe an. Der Freigabename wird dynamisch erstellt, wenn sich ein Benutzer mit seinem Home Directory verbindet, und hat die Form *windows_user_name*.

   > Sie können auch die `%u` Variable für die `-share-name` Option verwenden. Dies erstellt einen relativen Freigabepfad, der den zugeordneten UNIX-Benutzernamen verwendet.

   `-path %u` Gibt den relativen Pfad zum Home Directory an. Der relative Pfad wird dynamisch erstellt, wenn sich ein Benutzer mit seinem Home Directory verbindet, und hat die Form *mapped_UNIX_user_name*.

   > Der Wert für diese Option kann ebenfalls statische Elemente enthalten. Zum Beispiel `eng/%u`.

   `-share-properties homedirectory\[,...\]` Gibt die Eigenschaften dieser Freigabe an. Der `homedirectory` Wert muss angegeben werden. Zusätzliche Freigabeeigenschaften können mit einer durch Kommas getrennten Liste angegeben werden.
5. Es kann überprüft werden, ob die Freigabe die gewünschte Konfiguration aufweist, indem der `vserver cifs share show` Befehl verwendet wird.
6. Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` `vserver`Gibt die CIFS-fähige SVM an, zu der der Suchpfad hinzugefügt wird.

   `-path` `path`gibt den absoluten Verzeichnispfad zum Suchpfad an.
7. Es wird überprüft, ob der Suchpfad erfolgreich mit dem `vserver cifs home-directory search-path show` Befehl hinzugefügt wurde.
8. Falls der UNIX-Benutzer nicht existiert, kann der UNIX-Benutzer mit dem `vserver services unix-user create` Befehl erstellt werden.

   > Der UNIX-Benutzername, dem der Windows-Benutzername zugeordnet wird, muss vor der

Zuordnung des Benutzers existieren.

9. Eine Namenszuordnung für den Windows-Benutzer zum UNIX-Benutzer wird mit folgendem Befehl erstellt: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   Falls bereits Namenszuordnungen existieren, die Windows-Benutzer UNIX-Benutzern zuordnen, ist der Zuordnungsschritt nicht erforderlich.

   Der Windows-Benutzername wird dem entsprechenden UNIX-Benutzernamen zugeordnet. Wenn sich der Windows-Benutzer mit seiner Home Directory-Freigabe verbindet, erfolgt die Verbindung zu einem dynamisch erstellten Home Directory mit einem Freigabenamen, der dem Windows-Benutzernamen entspricht, ohne dass dem Benutzer bewusst ist, dass der Verzeichnisname dem UNIX-Benutzernamen entspricht.

10. Für Benutzer mit einem Home Directory wird ein entsprechendes Verzeichnis im Qtree oder Volume erstellt, das für die Aufnahme von Home Directories vorgesehen ist.

    Wenn beispielsweise ein Qtree mit dem Pfad `/vol/vol1/users` und dem zugeordneten UNIX-Benutzernamen des Benutzers, dessen Verzeichnis erstellt werden soll, „`unixuser1`“ ist, würde ein Verzeichnis mit folgendem Pfad erstellt: `/vol/vol1/users/unixuser1`.

    Wenn ein Volume mit dem Namen “home1” erstellt und unter `/home1` gemountet wurde, würde ein Verzeichnis mit folgendem Pfad erstellt: `/home1/unixuser1`.

11. Es wird überprüft, ob ein Benutzer erfolgreich eine Verbindung zum Home Share herstellen kann, entweder durch das Zuordnen eines Laufwerks oder durch das Verbinden über den UNC-Pfad.

    Wenn beispielsweise der Benutzer mydomain\user1 dem UNIX-Benutzer unixuser1 zugeordnet ist und eine Verbindung zu dem in Schritt 10 erstellten Verzeichnis auf SVM vs1 herstellen möchte, würde user1 die Verbindung über den UNC-Pfad `\\vs1\user1` herstellen.

Beispiel

Die Befehle im folgenden Beispiel erstellen eine Home Directory-Konfiguration mit den folgenden Einstellungen:

- Der Freigabename ist %w.
- Der relative Home Directory-Pfad ist %u.
- Der Suchpfad, der die Home-Verzeichnisse enthält, `/home1`, ist ein Volume, das mit dem UNIX-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM vs1 erstellt.

Diese Art von Home Directory-Konfiguration kann verwendet werden, wenn Benutzer sowohl von Windows-Hosts als auch von Windows- und UNIX-Hosts auf ihre Home Directories zugreifen und der Systemadministrator UNIX-basierte Benutzer und Gruppen verwendet, um den Zugriff auf das Dateisystem zu steuern.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Verwandte Informationen

- Home Directory-Konfigurationen mit den Variablen %w und %d erstellen
- Zusätzliche Home Directory-Konfigurationen werden erläutert.
- Informationen zu Home Directory-Pfaden von Benutzern anzeigen

Zusätzliche ONTAP SMB Home-Verzeichniskonfigurationen

Sie können zusätzliche Home-Verzeichniskonfigurationen mithilfe der `%w`, `%d` und `%u` Variablen erstellen, wodurch die Home-Verzeichniskonfiguration an Ihre Bedürfnisse

angepasst werden kann.

Sie können verschiedene Home-Verzeichnis-Konfigurationen erstellen, indem Sie Variablen und statische Zeichenketten in den Freigabenamen und Suchpfaden kombinieren. Die folgende Tabelle enthält einige Beispiele, die die Erstellung unterschiedlicher Home-Verzeichnis-Konfigurationen veranschaulichen:

Pfade, die erstellt werden, wenn `/vol1/user` Home-Verzeichnisse enthalten sind…	**Share-Befehl…**
Einen Freigabepfad erstellen `\\vs1\~win_username`, der den Benutzer zu `/vol1/user/win_username` führt	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Einen Freigabepfad erstellen `\\vs1\win_username`, der den Benutzer zu `/vol1/user/domain/win_username` führt	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Einen Freigabepfad erstellen `\\vs1\win_username`, der den Benutzer zu `/vol1/user/unix_username` führt	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Einen Freigabepfad erstellen `\\vs1\unix_username`, der den Benutzer zu `/vol1/user/unix_username` führt	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

ONTAP Befehle zur Verwaltung von SMB-Suchpfaden

Für die Verwaltung von Suchpfaden in SMB Home-Verzeichnis-Konfigurationen stehen spezielle ONTAP Befehle zur Verfügung. Beispielsweise gibt es Befehle zum Hinzufügen, Entfernen und Anzeigen von Informationen zu Suchpfaden. Es gibt auch einen Befehl zum Ändern der Reihenfolge des Suchpfads.

Wenn Sie möchten…	**Verwenden Sie diesen Befehl…**
Einen Suchpfad hinzufügen	`vserver cifs home-directory search-path add`
Suchpfade anzeigen	`vserver cifs home-directory search-path show`
Die Reihenfolge des Suchpfads ändern	`vserver cifs home-directory search-path reorder`
Einen Suchpfad entfernen	`vserver cifs home-directory search-path remove`

Weitere Informationen zu `vserver cifs home-directory search-path` finden sich in der "ONTAP-Befehlsreferenz".

Informationen zu den Home Directory-Pfaden von ONTAP SMB-Benutzern

Sie können den Home Directory-Pfad eines SMB-Benutzers auf der Storage Virtual Machine (SVM) anzeigen, was hilfreich ist, wenn mehrere CIFS-Home Directory-Pfade konfiguriert sind und nachvollzogen werden soll, welcher Pfad das Home Directory des Benutzers enthält.

Schritt

1. Der Home Directory-Pfad wird mit dem `vserver cifs home-directory show-user` Befehl angezeigt.

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  ----------------------
   vs1          user1                /home/user1
   ```

Verwandte Informationen

Zugänglichkeit zu Benutzer-Home-Verzeichnissen verwalten

Zugänglichkeit zu ONTAP SMB-Benutzer-Home-Verzeichnissen verwalten

Standardmäßig kann das Home-Verzeichnis eines Benutzers nur von diesem Benutzer selbst aufgerufen werden. Bei Freigaben, deren dynamischer Name mit einer Tilde (~) beginnt, lässt sich der Zugriff auf die Home-Verzeichnisse von Benutzern für Windows-Administratoren oder für beliebige andere Benutzer (öffentlicher Zugriff) aktivieren oder deaktivieren.

Bevor Sie beginnen

Die Home-Verzeichnisfreigaben auf der Storage Virtual Machine (SVM) müssen mit dynamischen Freigabenamen konfiguriert werden, denen eine Tilde (~) vorangestellt ist. Die folgenden Fälle veranschaulichen die Anforderungen an die Freigabebenennung:

Home-Verzeichnis-Freigabename	Beispiel für einen Befehl zum Herstellen einer Verbindung zur Freigabe
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Schritt

1. Die entsprechende Maßnahme ausführen:

Wenn der Zugriff auf die Home-Verzeichnisse der Benutzer aktiviert oder deaktiviert werden soll…	Geben Sie Folgendes ein…
Windows Administratoren	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` Der Standardwert ist `true`.
Jeder Benutzer (öffentlicher Zugriff)	a. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced` b. Zugriff aktivieren oder deaktivieren: `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public-enabled {true

Das folgende Beispiel ermöglicht den öffentlichen Zugriff auf die Home-Verzeichnisse der Benutzer:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Verwandte Informationen

Informationen zu Home Directory-Pfaden von Benutzern anzeigen

Konfiguration des SMB-Client-Zugriffs auf UNIX Symbol-Links

Informationen zur Bereitstellung von ONTAP SMB-Clientzugriff auf UNIX Symbol-Links

Ein Symbol-Link ist eine Datei, die in einer UNIX-Umgebung erstellt wird und einen Verweis auf eine andere Datei oder ein anderes Verzeichnis enthält. Wenn ein Client auf einen Symbol-Link zugreift, wird der Client zum Ziel der Datei oder des Verzeichnisses weitergeleitet, auf das sich der Symbol-Link bezieht. ONTAP unterstützt relative und absolute Symbol-Links, einschließlich Widelinks (absolute Links mit Zielen außerhalb des lokalen Dateisystems).

ONTAP bietet SMB-Clients die Möglichkeit, den auf der SVM konfigurierten UNIX Symbol-Links zu folgen. Diese Funktion ist optional und kann für jede Freigabe einzeln mit der `-symlink-properties` Option des `vserver cifs share create` Befehls mit einer der folgenden Einstellungen konfiguriert werden:

- Aktiviert mit lesen/schreiben Zugriff
- Aktiviert mit schreibgeschütztem Zugriff
- Deaktiviert durch Ausblenden von Symbol-Links für SMB-Clients
- Deaktiviert, kein Zugriff auf Symbol-Links von SMB-Clients

Wenn Sie Symbol-Links für eine Freigabe aktivieren, funktionieren relative Symbol-Links ohne weitere Konfiguration.

Wenn Sie Symbol-Links für eine Freigabe aktivieren, funktionieren absolute Symbol-Links nicht sofort. Zunächst muss eine Zuordnung zwischen dem UNIX-Pfad des Symbol-Link und dem Ziel-SMB-Pfad erstellt werden. Beim Erstellen von Zuordnungen absoluter Symbol-Links kann angegeben werden, ob es sich um

einen lokalen Link oder einen Widelink handelt; Widelinks können Links zu Dateisystemen auf anderen Speichersystemen oder zu Dateisystemen sein, die in separaten SVMs auf demselben ONTAP System gehostet werden. Beim Erstellen eines Widelinks müssen die Informationen enthalten sein, denen der Client folgen kann, das heißt, es wird ein Reparse-Point erstellt, damit der Client den Verbindungsordner erkennt. Wird ein absoluter Symbol-Link zu einer Datei oder einem Verzeichnis außerhalb der lokalen Freigabe erstellt, die Lokalität jedoch auf lokal gesetzt, verweigert ONTAP den Zugriff auf das Ziel.

> Wenn ein Client versucht, einen lokalen Symbol-Link (absolut oder relativ) zu löschen, wird nur der Symbol-Link gelöscht, nicht die Zieldatei oder das Zielverzeichnis. Wenn ein Client jedoch versucht, einen Widelink zu löschen, kann die tatsächliche Zieldatei oder das tatsächliche Zielverzeichnis gelöscht werden, auf das der Widelink verweist. ONTAP hat darauf keinen Einfluss, da der Client die Zieldatei oder das Zielverzeichnis außerhalb der SVM explizit öffnen und löschen kann.

- **Reparse Points und ONTAP Dateisystemdienste**

  Ein *Reparse-Point* ist ein NTFS-Dateisystemobjekt, das optional zusammen mit einer Datei auf Volumes gespeichert werden kann. Reparse-Points bieten SMB-Clients die Möglichkeit, erweiterte Dateisystemdienste zu erhalten, wenn sie mit Volumes im NTFS-Stil arbeiten. Reparse-Points bestehen aus Standard-Tags, die den Typ des Reparse-Points identifizieren, und dem Inhalt des Reparse-Points, der von SMB-Clients zur weiteren Verarbeitung durch den Client abgerufen werden kann. Von den Objekttypen, die für erweiterte Dateisystemfunktionen verfügbar sind, implementiert ONTAP die Unterstützung für NTFS-Symbol-Links und Verzeichnisverbindungspunkte mithilfe von Reparse-Point-Tags. SMB-Clients, die den Inhalt eines Reparse-Points nicht verstehen können, ignorieren ihn einfach und stellen den erweiterten Dateisystemdienst, den der Reparse-Point ermöglichen könnte, nicht bereit.

- **Verbindungspunkte für Verzeichnisse und ONTAP Unterstützung für Symbol-Links**

  Verzeichnis-Verbindungspunkte sind Stellen innerhalb der Verzeichnisstruktur eines Dateisystems, die auf alternative Speicherorte von Dateien verweisen können, entweder auf einem anderen Pfad (Symbol-Links) oder auf einem separaten Speichermedium (Widelinks). ONTAP SMB-Server stellen Windows-Clients Verzeichnis-Verbindungspunkte als Reparse Points zur Verfügung, wodurch fähige Clients beim Durchqueren eines Verzeichnis-Verbindungspunkts die Inhalte des Reparse Points von ONTAP abrufen können. Dadurch ist es möglich, zu verschiedenen Pfaden oder Speichermedien zu navigieren und eine Verbindung herzustellen, als wären sie Teil desselben Dateisystems.

- **Aktivieren der Widelink-Unterstützung mithilfe von Reparse-Point-Optionen**

  Die `-is-use-junctions-as-reparse-points-enabled` Option ist in ONTAP 9 standardmäßig aktiviert. Die Option zur Aktivierung der Information ist für jede Protokollversion konfigurierbar, da nicht alle SMB-Clients Widelinks unterstützen. Dadurch können Administratoren sowohl unterstützte als auch nicht unterstützte SMB-Clients berücksichtigen. Die Option `-widelink-as-reparse-point-versions` muss für jedes Clientprotokoll aktiviert werden, das über Widelinks auf die Freigabe zugreift; standardmäßig ist dies SMB1.

Verwandte Informationen

- "Windows-Sicherungsanwendungen und Unix-ähnliche Symbol-Links"
- "Microsoft Documentation: Analysepunkte"

Einschränkungen bei der Konfiguration von UNIX-Symbol-Links für ONTAP SMB-Zugriff

Bei der Konfiguration von UNIX-Symbol-Links für den SMB-Zugriff sind bestimmte Einschränkungen zu beachten.

Limit	Beschreibung
45	Maximale Länge des CIFS-Servernamens, die bei Verwendung eines FQDN für den CIFS-Servernamen angegeben werden kann. Alternativ kann der CIFS-Servername auch als NetBIOS-Name angegeben werden, der auf 15 Zeichen beschränkt ist.
80	Maximale Länge des Freigabenamens.
256	Maximale Länge des UNIX-Pfads, die beim Erstellen eines Symbol-Links oder beim Ändern des UNIX-Pfads eines bestehenden Symbol-Links angegeben werden kann. Der UNIX-Pfad muss mit einem “/” (slash) and end with a “/” beginnen. Sowohl der erste als auch der letzte Schrägstrich zählen zur 256-Zeichen-Grenze.
256	Maximale Länge des CIFS-Pfads, die beim Erstellen eines Symbol-Links oder beim Ändern des CIFS-Pfads eines bestehenden Symbol-Links angegeben werden kann. Der CIFS-Pfad muss mit einem “/” (slash) and end with a “/” beginnen. Sowohl der erste als auch der letzte Schrägstrich zählen zur 256-Zeichen-Grenze.

Verwandte Informationen

Symbol-Link-Zuordnungen für Shares erstellen

Automatische DFS-Ankündigungen auf ONTAP SMB-Servern steuern

Eine CIFS-Serveroption steuert, wie DFS-Funktionen SMB-Clients beim Zugriff auf Freigaben mitgeteilt werden. Da ONTAP DFS-Verweise verwendet, wenn Clients über SMB auf Symbol-Links zugreifen, ist es wichtig, die Auswirkungen der Deaktivierung oder Aktivierung dieser Option zu kennen.

Eine CIFS-Serveroption legt fest, ob die CIFS-Server SMB-Clients automatisch ihre DFS-Fähigkeit signalisieren. Standardmäßig ist diese Option aktiviert und der CIFS-Server signalisiert SMB-Clients immer seine DFS-Fähigkeit (auch beim Zugriff auf Freigaben, bei denen der Zugriff auf Symbol-Links deaktiviert ist). Wenn der CIFS-Server seine DFS-Fähigkeit nur dann signalisieren soll, wenn Clients auf Freigaben zugreifen, bei denen der Zugriff auf Symbol-Links aktiviert ist, kann diese Option deaktiviert werden.

Es ist zu beachten, was passiert, wenn diese Option deaktiviert ist:

- Die Freigabekonfigurationen für Symbol-Links bleiben unverändert.
- Wenn der Freigabeparameter so eingestellt ist, dass der Zugriff auf Symbol-Links (entweder Lese- und Schreibzugriff oder nur Lesezugriff) erlaubt ist, gibt der CIFS-Server gegenüber Clients, die eine Verbindung zu dieser Freigabe herstellen, DFS-Funktionen bekannt.

  Clientverbindungen und der Zugriff auf Symbol-Links erfolgen ohne Unterbrechung.

- Wenn der Freigabeparameter so eingestellt ist, dass der Zugriff auf Symbol-Links nicht zulässig ist (entweder durch Deaktivierung des Zugriffs oder wenn der Wert für den Freigabeparameter null ist), gibt der CIFS-Server gegenüber Clients, die eine Verbindung zu dieser Freigabe herstellen, keine DFS-Funktionen bekannt.

  Da Clients Informationen zwischengespeichert haben, dass der CIFS-Server DFS-fähig ist und er dies nicht mehr bekannt gibt, können Clients, die mit Freigaben verbunden sind, bei denen der Symbol-Link-Zugriff deaktiviert ist, nach Deaktivierung der CIFS-Server-Option möglicherweise nicht mehr auf diese Freigaben zugreifen. Nach Deaktivierung der Option kann es erforderlich sein, die mit diesen Freigaben verbundenen Clients neu zu starten, wodurch die zwischengespeicherten Informationen gelöscht werden.

Diese Änderungen gelten nicht für SMB 1.0 Verbindungen.

Konfiguration der UNIX-Unterstützung für Symbol-Links auf ONTAP SMB-Freigaben

Sie können die Unterstützung für UNIX Symbol-Links auf SMB-Freigaben konfigurieren, indem Sie beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern bestehender SMB-Freigaben eine Symbol-Link Freigabeeigenschaft festlegen. Die Unterstützung für UNIX Symbol-Links ist standardmäßig aktiviert. Die Unterstützung für UNIX Symbol-Links kann auf einer Freigabe auch deaktiviert werden.

Über diese Aufgabe

Bei der Konfiguration der UNIX Symbol-Link-Unterstützung für SMB-Freigaben steht eine der folgenden Einstellungen zur Auswahl:

Einstellung	Beschreibung
`enable` (VERALTET*)	Gibt an, dass Symbol-Links für Lese- und Schreibzugriffe aktiviert sind.
`read_only` (VERALTET*)	Legt fest, dass Symbol-Links für den Nur-Lese-Zugriff aktiviert sind. Diese Einstellung gilt nicht für Widelinks. Widelink-Zugriff ist immer Lese- und Schreibzugriff.
`hide` (VERALTET*)	Legt fest, dass SMB-Clients keine Symbol-Links sehen können.
`no-strict-security`	Legt fest, dass Clients Symbol-Links außerhalb der Freigabegrenzen folgen.
`symlinks`	Gibt an, dass Symbol-Links lokal für Lese- und Schreibzugriffe aktiviert sind. Die DFS-Ankündigungen werden nicht generiert, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf `true` gesetzt ist. Dies ist die Standardeinstellung.
`symlinks-and-widelinks`	Gibt an, dass sowohl lokale Symbol-Links als auch Widelinks für Lese- und Schreibzugriffe verwendet werden. Die DFS-Ankündigungen werden sowohl für lokale Symbol-Links als auch für Widelinks generiert, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf `false` gesetzt ist.

Einstellung	Beschreibung
`disable`	Gibt an, dass Symbol-Links und Widelinks deaktiviert sind. Die DFS-Ankündigungen werden nicht generiert, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf `true` gesetzt ist.
"" (null, nicht gesetzt)	Deaktiviert Symbol-Links auf der Freigabe.
– (nicht festgelegt)	Deaktiviert Symbol-Links auf der Freigabe.

*Die Parameter *enable*, *hide* und *read-only* sind veraltet und werden möglicherweise in einer zukünftigen Version von ONTAP entfernt.

Schritte

1. Symbol-Link-Unterstützung konfigurieren oder deaktivieren:

Wenn dies der Fall ist…	Eingeben…
Eine neue SMB-Freigabe	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Eine bestehende SMB-Freigabe
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Es sollte überprüft werden, ob die SMB-Freigabekonfiguration korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Der folgende Befehl erstellt eine SMB-Freigabe mit dem Namen “data1”, wobei die UNIX-Symbol-Link-Konfiguration auf `enable`gesetzt ist:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
```

```
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                            Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: -
      Directory Mode Creation Mask: -
                     Share Comment: -
                         Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                       Volume Name: -
                     Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Verwandte Informationen

Symbol-Link-Zuordnungen für Shares erstellen

Symbol-Link-Zuordnungen für ONTAP SMB-Freigaben erstellen

Sie können Zuordnungen von UNIX-Symbol-Links für SMB-Freigaben erstellen. Es ist möglich, entweder einen relativen Symbol-Link zu erstellen, der auf die Datei oder den Ordner relativ zu seinem übergeordneten Ordner verweist, oder einen absoluten Symbol-Link, der auf die Datei oder den Ordner über einen absoluten Pfad verweist.

Über diese Aufgabe

Widelinks sind von Mac OS X Clients aus nicht zugänglich, wenn Sie SMB 2.x verwenden. Wenn ein Benutzer versucht, über Widelinks von einem Mac OS X Client eine Verbindung zu einer Freigabe herzustellen, schlägt der Versuch fehl. Widelinks können jedoch mit Mac OS X Clients verwendet werden, wenn Sie SMB 1 verwenden.

Schritte

1. Symbol-Link-Zuordnungen für SMB-Freigaben erstellen: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

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

   `-unix-path path` gibt den UNIX-Pfad an. Der UNIX-Pfad muss mit einem Schrägstrich (`/` beginnen und mit einem Schrägstrich (`/` enden.

   `-share-name share_name` Gibt den Namen der zuzuordnenden SMB-Freigabe an.

   `-cifs-path path` gibt den CIFS-Pfad an. Der CIFS-Pfad muss mit einem Schrägstrich (`/` beginnen und

mit einem Schrägstrich (`/` enden.

`-cifs-server server_name`Gibt den Namen des CIFS-Servers an. Der Name des CIFS-Servers kann als DNS-Name (zum Beispiel mynetwork.cifs.server.com), IP-Adresse oder NetBIOS-Name angegeben werden. Der NetBIOS-Name kann mit dem `vserver cifs show` Befehl ermittelt werden. Wenn dieser optionale Parameter nicht angegeben wird, ist der Standardwert der NetBIOS-Name des lokalen CIFS-Servers.

`-locality local|free|widelink}` gibt an, ob ein lokaler Link, ein freier Link oder ein breiter Symbol-Link erstellt wird. Ein lokaler Symbol-Link verweist auf die lokale SMB-Freigabe. Ein freier Symbol-Link kann auf eine beliebige Stelle auf dem lokalen SMB-Server verweisen. Ein breiter Symbol-Link verweist auf eine beliebige SMB-Freigabe im Netzwerk. Wird dieser optionale Parameter nicht angegeben, ist der Standardwert `local`.

`-home-directory true false}` gibt an, ob die Zielfreigabe ein Home-Verzeichnis ist. Auch wenn dieser Parameter optional ist, muss dieser Parameter auf `true` gesetzt werden, wenn die Zielfreigabe als Home-Verzeichnis konfiguriert ist. Der Standardwert ist `false`.

Beispiel

Der folgende Befehl erstellt eine Symbol-Link-Zuordnung auf der SVM mit dem Namen vs1. Sie enthält den UNIX-Pfad `/src/`, den SMB-Freigabenamen “SOURCE”, den CIFS-Pfad `/mycompany/source/` und die CIFS-Server-IP-Adresse 123.123.123.123 und ist ein Widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Verwandte Informationen

UNIX Symbol-Link-Unterstützung auf Freigaben konfigurieren

ONTAP Befehle zur Verwaltung von SMB Symbol-Link-Zuordnungen

Es gibt spezielle ONTAP Befehle zur Verwaltung von Symbol-Link-Zuordnungen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen einer Symbol-Link-Zuordnung	`vserver cifs symlink create`
Informationen zu Symbol-Link-Zuordnungen anzeigen	`vserver cifs symlink show`
Eine Symbol-Link-Zuordnung ändern	`vserver cifs symlink modify`
Symbol-Link-Zuordnung löschen	`vserver cifs symlink delete`

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

Windows-Sicherungsanwendungen und Unix-ähnliche Symbol-Links auf ONTAP SMB-Servern

Wenn eine unter Windows laufende Backup-Anwendung auf einen Symbol-Link (Symlink) im Unix-Stil stößt, wird diesem gefolgt und die Daten werden gesichert. Ab ONTAP 9.15.1 besteht die Möglichkeit, anstelle der Daten die Symlinks selbst zu sichern. Diese

Funktion wird mit ONTAP FlexGroup Volumes und FlexVols vollständig unterstützt.

Überblick

Bevor Sie ändern, wie ONTAP Symbol-Links während einer Windows-Sicherung verarbeitet, sollten Ihnen die Vorteile, die wichtigsten Konzepte und die Konfigurationsoptionen bekannt sein.

Vorteile

Wenn diese Funktion deaktiviert oder nicht verfügbar ist, wird jeder Symbol-Link durchlaufen und die Daten, auf die er verweist, werden gesichert. Dadurch können mitunter unnötige Daten gesichert werden und in bestimmten Fällen kann die Anwendung in einer Schleife enden. Die Sicherung der Symbol-Links selbst vermeidet diese Probleme. Da die Symbol-Link-Dateien im Vergleich zu den Daten in den meisten Fällen sehr klein sind, ist die Sicherung zudem schneller abgeschlossen. Die Gesamtleistung des Clusters kann sich aufgrund der reduzierten IO-Operationen ebenfalls verbessern.

Windows Server Umgebung

Diese Funktion wird von Sicherungsanwendungen unter Windows unterstützt. Die relevanten technischen Aspekte der Umgebung sollten vor der Verwendung bekannt sein.

Erweiterte Attribute

Windows unterstützt erweiterte Attribute (EA), die zusammen zusätzliche Metadaten bilden, die optional mit den Dateien verknüpft sind. Diese Attribute werden von verschiedenen Anwendungen verwendet, wie zum Beispiel vom Windows Subsystem for Linux, wie unter "Dateiberechtigungen für WSL" beschrieben. Anwendungen können beim Lesen von Daten aus ONTAP erweiterte Attribute für jede Datei anfordern.

Die symbolischen Verknüpfungen werden in den erweiterten Attributen zurückgegeben, wenn die Funktion aktiviert ist. Daher muss eine Sicherungsanwendung standardmäßige Unterstützung für erweiterte Attribute bieten, die zum Speichern der Metadaten verwendet wird. Einige Windows-Dienstprogramme unterstützen und bewahren die erweiterten Attribute. Wenn die Sicherungssoftware jedoch das Sichern und Wiederherstellen der erweiterten Attribute nicht unterstützt, werden die Metadaten, die mit jeder Datei verknüpft sind, nicht erhalten und die symbolischen Verknüpfungen werden nicht korrekt verarbeitet.

Windows Konfiguration

Backup-Anwendungen, die auf einem Microsoft Windows-Server ausgeführt werden, können eine spezielle Berechtigung erhalten, die es ihnen ermöglicht, die normale Dateisicherheit zu umgehen. Dies erfolgt typischerweise durch das Hinzufügen der Anwendungen zur Gruppe Backup Operators. Die Anwendungen können dann Dateien nach Bedarf sichern und wiederherstellen sowie weitere zugehörige Systemoperationen ausführen. Es gibt subtile Änderungen am von den Backup-Anwendungen verwendeten SMB-Protokoll, die von ONTAP beim Lesen und Schreiben der Daten erkannt werden können.

Anforderungen

Die Symlink Backup-Funktion hat mehrere Anforderungen, darunter:

- Auf Ihrem Cluster läuft ONTAP 9.15.1 oder höher.
- Eine Windows-Sicherungsanwendung, der spezielle Sicherungsberechtigungen zugewiesen wurden.
- Die Backup-Anwendung muss außerdem erweiterte Attribute unterstützen und diese während der Backup-Vorgänge anfordern.
- Die ONTAP Symlink Backup-Funktion ist für die entsprechende Daten-SVM aktiviert.

Konfigurationsoptionen

Zusätzlich zur ONTAP CLI kann diese Funktion auch über die ONTAP REST API verwaltet werden. Siehe "Neues zur ONTAP REST API und Automatisierung" für weitere Informationen. Die Konfiguration, die festlegt, wie ONTAP die Unix-Style-Symbol-Links verarbeitet, muss für jede SVM separat vorgenommen werden.

Die Symlink-Backup-Funktion in ONTAP aktivieren

Mit ONTAP 9.15.1 wurde eine Konfigurationsoption für einen bestehenden CLI-Befehl eingeführt. Mit dieser Option lässt sich die Verarbeitung von Unix-ähnlichen Symlinks aktivieren oder deaktivieren.

Bevor Sie beginnen

Die grundlegenden Anforderungen sollten überprüft werden. Zusätzlich:

- Die Möglichkeit besteht, die CLI-Berechtigungen auf die fortgeschrittene Stufe anzuheben.
- Bestimmen Sie die Daten-SVM, die Sie modifizieren möchten. Die SVM `vs1` wird im Beispielbefehl verwendet.

Schritte

1. Die erweiterte Berechtigungsstufe wird festgelegt.

```
set privilege advanced
```

2. Symlink-Dateisicherung aktivieren.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Erfahren Sie mehr über BranchCache

Informationen zur Verwendung von BranchCache zum Zwischenspeichern von ONTAP SMB-Freigabeinhalten in einer Zweigstelle

BranchCache wurde von Microsoft entwickelt, um das Zwischenspeichern von Inhalten auf Rechnern lokal zu den anfragenden Clients zu ermöglichen. Die ONTAP Implementierung von BranchCache kann die Auslastung des Weitverkehrsnetzes (WAN) reduzieren und eine verbesserte Zugriffszeit bieten, wenn Benutzer in einer Zweigstelle über SMB auf Inhalte zugreifen, die auf Storage Virtual Machines (SVMs) gespeichert sind.

Wenn BranchCache konfiguriert wird, rufen Windows BranchCache-Clients Inhalte zunächst von der SVM ab und speichern die Inhalte anschließend auf einem Computer innerhalb der Zweigstelle im Cache. Fordert ein anderer BranchCache-fähiger Client in der Zweigstelle dieselben Inhalte an, authentifiziert und autorisiert die SVM zunächst den anfragenden Benutzer. Anschließend prüft die SVM, ob die zwischengespeicherten Inhalte noch aktuell sind, und sendet dem Client, falls dies zutrifft, Metadaten zu den zwischengespeicherten Inhalten. Der Client verwendet dann die Metadaten, um die Inhalte direkt aus dem lokal gespeicherten Cache abzurufen.

Verwandte Informationen

Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von Dateien für die Offline-

Nutzung zu ermöglichen

Informationen zur Unterstützung von ONTAP SMB BranchCache Versionen

Sie sollten wissen, welche BranchCache Versionen ONTAP unterstützt.

ONTAP unterstützt BranchCache 1 und die erweiterte BranchCache 2:

- Wenn BranchCache auf dem SMB-Server für die Storage Virtual Machine (SVM) konfiguriert wird, kann BranchCache 1, BranchCache 2 oder alle Versionen aktiviert werden.

  Standardmäßig sind alle Versionen aktiviert.

- Wenn Sie nur BranchCache 2 aktivieren, müssen die Windows-Clientrechner im Remote-Büro BranchCache 2 unterstützen.

  Nur SMB 3.0 oder neuere Clients unterstützen BranchCache 2.

Weitere Informationen zu BranchCache Versionen finden sich in der Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informationen zu den Anforderungen an die Unterstützung des ONTAP SMB Netzwerkprotokolls

Es ist wichtig, die Anforderungen an das Netzwerkprotokoll für die Implementierung von ONTAP BranchCache zu kennen.

Die ONTAP BranchCache Funktion kann über IPv4- und IPv6-Netzwerke mit SMB 2.1 oder höher implementiert werden.

Alle CIFS-Server und Rechner in Zweigstellen, die an der BranchCache-Implementierung beteiligt sind, müssen das SMB 2.1 oder eine spätere Protokollversion aktiviert haben. SMB 2.1 verfügt über Protokollerweiterungen, die es einem Client ermöglichen, an einer BranchCache-Umgebung teilzunehmen. Dies ist die minimale SMB-Protokollversion, die BranchCache unterstützt. SMB 2.1 unterstützt BranchCache Version 1.

Wenn BranchCache Version 2 verwendet werden soll, ist SMB 3.0 die minimal unterstützte Version. Alle CIFS-Server und Rechner in Zweigstellen, die an einer BranchCache 2-Implementierung beteiligt sind, müssen SMB 3.0 oder höher aktiviert haben.

Wenn Sie über Außenstellen verfügen, in denen einige der Clients nur SMB 2.1 und andere der Clients SMB 3.0 unterstützen, kann auf dem CIFS-Server eine BranchCache Konfiguration implementiert werden, die Caching-Unterstützung sowohl für BranchCache 1 als auch für BranchCache 2 bietet.

> Auch wenn die Microsoft BranchCache Funktion sowohl die Verwendung der HTTP/HTTPS- als auch der SMB-Protokolle als Dateizugriffsprotokolle unterstützt, unterstützt ONTAP BranchCache nur die Verwendung von SMB.

Informationen zu den Versionsanforderungen für ONTAP SMB und Windows Hosts

ONTAP und Windows-Hosts in Zweigstellen müssen bestimmte Versionsanforderungen erfüllen, bevor BranchCache konfiguriert werden kann.

Vor der Konfiguration von BranchCache muss sichergestellt werden, dass die Version von ONTAP auf dem Cluster und den beteiligten Zweigstellen-Clients SMB 2.1 oder höher sowie die BranchCache-Funktion unterstützt. Bei Konfiguration des Hosted Cache-Modus ist außerdem sicherzustellen, dass ein unterstützter Host für den Cache-Server verwendet wird.

BranchCache 1 wird auf den folgenden ONTAP Versionen und Windows Hosts unterstützt:

- Content Server: Storage Virtual Machine (SVM) mit ONTAP
- Cache Server: Windows Server 2008 R2 oder Windows Server 2012 oder höher
- Peer oder Client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 oder Windows Server 2012 oder höher

BranchCache 2 wird auf den folgenden ONTAP Versionen und Windows Hosts unterstützt:

- Content Server: SVM mit ONTAP
- Cache Server: Windows Server 2012 oder höher
- Peer oder Client: Windows 8 oder Windows Server 2012 oder höher

Informationen zu den Gründen, aus denen ONTAP SMB BranchCache-Hashes für ungültig erklärt

Das Verständnis der Gründe, warum ONTAP Hashes ungültig macht, kann bei der Planung Ihrer BranchCache Konfiguration hilfreich sein. Dies kann bei der Entscheidung unterstützen, welchen Betriebsmodus konfiguriert werden sollte, und bei der Auswahl helfen, auf welchen Freigaben BranchCache aktiviert werden soll.

ONTAP muss BranchCache-Hashwerte verwalten, um sicherzustellen, dass die Hashwerte gültig sind. Ist ein Hashwert ungültig, erklärt ONTAP den Hashwert für ungültig und berechnet beim nächsten Anfordern desselben Inhalts einen neuen Hashwert, sofern BranchCache weiterhin aktiviert ist.

ONTAP macht Hashes aus folgenden Gründen ungültig:

- Der Serverschlüssel wurde geändert.

  Wenn der Serverschlüssel geändert wird, macht ONTAP alle Hashes im Hash-Speicher ungültig.

- Ein Hashwert wird aus dem Cache gelöscht, da die maximale Größe des BranchCache Hashspeichers erreicht wurde.

  Dies ist ein anpassbarer Parameter und kann entsprechend Ihren Geschäftsanforderungen geändert werden.

- Eine Datei wird entweder über SMB- oder NFS-Zugriff geändert.
- Eine Datei, für die berechnete Hashwerte vorliegen, wird mit dem `snap restore` Befehl wiederhergestellt.
- Ein Volume, das SMB-Freigaben enthält, die für BranchCache aktiviert sind, wird mit dem `snap restore` Befehl wiederhergestellt.

Informationen zur Auswahl des ONTAP SMB Hash-Speicherorts

Bei der Konfiguration von BranchCache wählen Sie aus, wo die Hashwerte gespeichert werden und wie groß der Hashspeicher sein soll. Das Verständnis der Richtlinien bei der

Auswahl von Speicherort und Größe des Hashspeichers kann bei der Planung der BranchCache-Konfiguration auf einer CIFS-fähigen SVM unterstützen.

- Der Hash-Speicher sollte auf einem Volume platziert werden, auf dem atime-Aktualisierungen zulässig sind.

  Die Zugriffszeit einer Hash-Datei wird verwendet, um häufig genutzte Dateien im Hash-Speicher zu halten. Wenn atime-Aktualisierungen deaktiviert sind, wird die Erstellungszeit zu diesem Zweck verwendet. Es ist vorzuziehen, atime zur Nachverfolgung häufig genutzter Dateien zu verwenden.

- Hashwerte können nicht auf schreibgeschützten Dateisystemen wie SnapMirror Destinationen und SnapLock Volumes gespeichert werden.
- Wenn die maximale Größe des Hash-Speichers erreicht ist, werden ältere Hashes entfernt, um Platz für neue Hashes zu schaffen.

  Sie können die maximale Größe des Hash-Speichers erhöhen, um die Anzahl der aus dem Cache gelöschten Hashes zu reduzieren.

- Wenn das Volume, auf dem Sie Hashes speichern, nicht verfügbar oder voll ist oder wenn ein Problem mit der Kommunikation innerhalb des Clusters besteht, sodass der BranchCache-Dienst keine Hash-Informationen abrufen kann, sind BranchCache-Dienste nicht verfügbar.

  Das Volume ist möglicherweise nicht verfügbar, weil es offline ist oder weil der Speicheradministrator einen neuen Speicherort für den Hash Store angegeben hat.

  Dies führt nicht zu Problemen beim Dateizugriff. Falls der Zugriff auf den Hash-Speicher behindert wird, gibt ONTAP einen von Microsoft definierten Fehler an den Client zurück, woraufhin der Client die Datei über die normale SMB-Leseanforderung anfordert.

Verwandte Informationen

- BranchCache auf Servern konfigurieren
- Konfigurationen von BranchCache auf Freigaben ändern

Empfehlungen zu ONTAP SMB BranchCache

Bevor Sie BranchCache konfigurieren, sollten bestimmte Empfehlungen berücksichtigt werden, wenn entschieden wird, bei welchen SMB-Freigaben das BranchCache-Caching aktiviert werden soll.

Die folgenden Empfehlungen sind bei der Entscheidung zu berücksichtigen, welchen Betriebsmodus Sie verwenden und auf welchen SMB-Freigaben Sie BranchCache aktivieren:

- Die Vorteile von BranchCache sind reduziert, wenn sich die remote zwischengespeicherten Daten häufig ändern.
- BranchCache-Dienste sind vorteilhaft für Freigaben, die Dateiinhalte enthalten, die von mehreren Remote-Office-Clients wiederverwendet werden, oder für Dateiinhalte, auf die ein einzelner Remote-Benutzer wiederholt zugreift.
- Das Aktivieren des Cachings für schreibgeschützte Inhalte wie Daten in Snapshots und SnapMirror-Zielen kann in Betracht gezogen werden.

Konfiguration von BranchCache auf ONTAP SMB-Servern

Um BranchCache zu verwenden, müssen Sie Ihre Clients und, falls erforderlich, die gehosteten Cache-Server in Zweigstellen konfigurieren, in denen Inhalte zwischengespeichert werden. Sie können BranchCache für einzelne Freigaben oder für alle SMB-Freigaben konfigurieren. Wenn Sie die Konfiguration pro Freigabe wählen, müssen Sie BranchCache auf jeder SMB-Freigabe aktivieren, die Caching bereitstellen soll. Sie können BranchCache auch so einstellen, dass das Caching automatisch auf allen SMB-Freigaben aktiviert wird.

Bevor Sie beginnen

Die folgenden Voraussetzungen müssen erfüllt sein, bevor BranchCache auf dem CIFS-Server für Ihre SVM konfiguriert wird:

- ONTAP muss auf allen Knoten im Cluster installiert sein.
- CIFS muss lizenziert und ein SMB-Server konfiguriert 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.
- IPv4- oder IPv6-Netzwerkkonnektivität muss konfiguriert werden.
- Für BranchCache 1 muss SMB 2.1 oder höher aktiviert sein.
- Für BranchCache 2 muss SMB 3.0 aktiviert sein und die Remote-Windows-Clients müssen BranchCache 2 unterstützen.

Über diese Aufgabe

Sie können BranchCache auf SVMs konfigurieren.

- Es kann eine All-Shares-BranchCache Konfiguration erstellt werden, wenn Caching-Dienste für alle Inhalte angeboten werden sollen, die in allen SMB-Freigaben auf dem CIFS-Server enthalten sind.
- Eine BranchCache Konfiguration pro Freigabe kann erstellt werden, um Caching-Dienste für Inhalte bereitzustellen, die sich in ausgewählten SMB-Freigaben auf dem CIFS-Server befinden.

Die folgenden Parameter müssen bei der Konfiguration von BranchCache angegeben werden:

Erforderliche Parameter	Beschreibung
SVM Name	BranchCache ist auf SVM-Basis konfiguriert. Es muss angegeben werden, auf welcher CIFS-aktivierten SVM der BranchCache-Dienst konfiguriert werden soll.
Pfad zum Hash-Store	BranchCache-Hashwerte werden in regulären Dateien auf dem SVM-Volume gespeichert. Der Pfad zu einem vorhandenen Verzeichnis, in dem ONTAP die Hashdaten speichern soll, muss angegeben werden. Der BranchCache-Hashpfad muss les- und schreibbar sein. Schreibgeschützte Pfade, wie beispielsweise Snapshot-Verzeichnisse, sind nicht zulässig. Hashdaten können auf einem Volume gespeichert werden, das bereits andere Daten enthält, oder es kann ein separates Volume zur Speicherung der Hashdaten erstellt werden. Wenn es sich bei der SVM um eine SVM-Notfallwiederherstellungsquelle handelt, darf sich der Hash-Pfad nicht auf dem Root Volume befinden. Dies liegt daran, dass das Root Volume nicht auf das Notfallwiederherstellungsziel repliziert wird. Der Hash-Pfad kann Leerzeichen und alle gültigen Dateinamenzeichen enthalten.

Sie können optional die folgenden Parameter angeben:

Optionale Parameter	Beschreibung
Unterstützte Versionen	ONTAP unterstützt BranchCache 1 und 2. Es ist möglich, Version 1, Version 2 oder beide Versionen zu aktivieren. Standardmäßig sind beide Versionen aktiviert.
Maximale Größe des Hash-Speichers	Sie können die Größe des Hash-Datenspeichers festlegen. Wenn die Hash-Daten diesen Wert überschreiten, löscht ONTAP ältere Hashes, um Platz für neuere Hashes zu schaffen. Die Standardgröße für den Hash-Speicher beträgt 1 GB. BranchCache arbeitet effizienter, wenn Hashes nicht in übermäßigem Maße verworfen werden. Wenn festgestellt wird, dass Hashes häufig verworfen werden, weil der Hash-Speicher voll ist, kann die Größe des Hash-Speichers durch Anpassen der BranchCache-Konfiguration erhöht werden.
Serverschlüssel	Sie können einen Serverschlüssel festlegen, den der BranchCache-Dienst verwendet, um zu verhindern, dass Clients sich als der BranchCache-Server ausgeben. Wenn Sie keinen Serverschlüssel angeben, wird beim Erstellen der BranchCache-Konfiguration ein zufälliger generiert. Sie können den Serverschlüssel auf einen bestimmten Wert setzen, sodass, falls mehrere Server BranchCache-Daten für dieselben Dateien bereitstellen, Clients Hashes von jedem Server mit demselben Serverschlüssel verwenden können. Enthält der Serverschlüssel Leerzeichen, muss er in Anführungszeichen gesetzt werden.
Betriebsart	Standardmäßig ist BranchCache für jede Freigabe einzeln aktiviert. • Um eine BranchCache Konfiguration zu erstellen, bei der BranchCache pro Freigabe aktiviert wird, kann entweder dieser optionale Parameter nicht angegeben werden oder `per-share` angegeben werden. • Um BranchCache auf allen Freigaben automatisch zu aktivieren, muss der Betriebsmodus auf `all-shares` gesetzt werden.

Schritte

1. SMB 2.1 und 3.0 nach Bedarf aktivieren:
   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

      ```
      set -privilege advanced
      ```

   b. Überprüfen Sie die konfigurierten SVM-SMB-Einstellungen, um festzustellen, ob alle benötigten SMB-Versionen aktiviert sind:

      ```
      vserver cifs options show -vserver <SVM_name>
      ```

   c. Aktivieren Sie gegebenenfalls SMB 2.1:

      ```
      vserver cifs options modify -vserver <SVM_name> -smb2-enabled true
      ```

      Der Befehl aktiviert sowohl SMB 2.0 als auch SMB 2.1.

d. Aktivieren Sie gegebenenfalls SMB 3.0:

```
vserver cifs options modify -vserver <SVM_name> -smb3-enabled true
```

e. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

2. Konfigurieren BranchCache:

```
vserver cifs branchcache create -vserver <SVM_name> -hash-store-path
<path> [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-
enable|v2-enable|enable-all}] [-server-key <text>] -operating-mode {per-
share|all-shares}
```

Der angegebene Hash-Speicherpfad muss existieren und sich auf einem vom SVM verwalteten Volume befinden. Der Pfad muss außerdem auf einem beschreibbaren Volume liegen. Der Befehl schlägt fehl, wenn der Pfad schreibgeschützt ist oder nicht existiert.

Wenn Sie denselben Serverschlüssel für zusätzliche SVM BranchCache Konfigurationen verwenden möchten, sollte der eingegebene Wert für den Serverschlüssel festgehalten werden. Der Serverschlüssel wird nicht angezeigt, wenn Informationen zur BranchCache Konfiguration angezeigt werden.

3. Überprüfen Sie, ob die BranchCache-Konfiguration korrekt ist:

```
vserver cifs branchcache show -vserver <SVM_name>
```

Beispiele

Die folgenden Befehle überprüfen, ob sowohl SMB 2.1 als auch 3.0 aktiviert sind, und konfigurieren BranchCache, um das Caching auf allen SMB-Freigaben auf SVM vs1 automatisch zu aktivieren:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin
```

```
cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Die folgenden Befehle überprüfen, ob sowohl SMB 2.1 als auch 3.0 aktiviert sind, konfigurieren BranchCache, um die Zwischenspeicherung pro Freigabe auf SVM vs1 zu ermöglichen, und überprüfen die BranchCache-Konfiguration:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Was kommt als Nächstes?

Nach der Konfiguration von BranchCache auf dem SMB-Server ist BranchCache auf den Clientcomputern und optional auf den Caching-Servern in der Außenstelle zu installieren und zu konfigurieren. Microsoft stellt Anweisungen für die Konfiguration von BranchCache in der Außenstelle bereit.

Anweisungen zur Konfiguration von Clients für Zweigstellen und optional von Caching-Servern zur Nutzung von BranchCache sind auf der Microsoft BranchCache Web Site verfügbar.

"Microsoft BranchCache Docs: Was ist neu?"

Verwandte Informationen

- Informationen zur Unterstützung von BranchCache-Versionen
- Eine SMB-Freigabe mit aktiviertem BranchCache erstellen
- BranchCache auf bestehenden Freigaben aktivieren
- Konfigurationen von BranchCache auf Freigaben ändern
- Informationen zum Deaktivieren von BranchCache auf Freigaben
- Die BranchCache Konfiguration auf Freigaben löschen

Aktivieren und Deaktivieren von BranchCache

Informationen zur Konfiguration von BranchCache-fähigen ONTAP SMB-Freigaben

Nachdem BranchCache auf dem SMB-Server und in der Zweigstelle konfiguriert wurde, kann BranchCache auf SMB-Freigaben aktiviert werden, die Inhalte enthalten, die Clients in den Zweigstellen zwischenspeichern dürfen.

BranchCache-Caching kann für alle SMB-Freigaben auf dem SMB-Server oder für einzelne Freigaben aktiviert werden.

- Wenn BranchCache für einzelne Freigaben aktiviert wird, kann BranchCache entweder beim Erstellen der Freigabe oder durch Ändern bestehender Freigaben aktiviert werden.

  Wenn das Caching für eine bestehende SMB-Freigabe aktiviert wird, beginnt ONTAP mit der Berechnung von Hashwerten und dem Senden von Metadaten an Clients, die Inhalte anfordern, sobald BranchCache auf dieser Freigabe aktiviert wird.

- Clients, die bereits eine SMB-Verbindung zu einer Freigabe haben, erhalten keine BranchCache-Unterstützung, wenn BranchCache anschließend für diese Freigabe aktiviert wird.

  ONTAP signalisiert BranchCache Unterstützung für eine Freigabe beim Einrichten der SMB-Sitzung. Clients, die bereits Sitzungen aufgebaut haben, wenn BranchCache aktiviert wird, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe nutzen zu können.

> Wenn BranchCache auf einer SMB-Freigabe anschließend deaktiviert wird, stellt ONTAP das Senden von Metadaten an den anfragenden Client ein. Ein Client, der Daten benötigt, ruft diese direkt vom Content-Server (SMB-Server) ab.

Aktivieren Sie BranchCache für neue SMB-Freigaben

Sie können BranchCache auf einer SMB-Freigabe aktivieren, wenn Sie die Freigabe erstellen, indem Sie die `branchcache` Freigabeeigenschaft festlegen.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Offline-Dateikonfiguration der Freigabe auf manuelles Caching eingestellt sein.

  Dies ist die Standardeinstellung beim Erstellen einer Freigabe.

- Sie können beim Erstellen der BranchCache-aktivierten Freigabe auch zusätzliche optionale Freigabeparameter angeben.
- Sie können die `branchcache`Eigenschaft für eine Freigabe festlegen, selbst wenn BranchCache auf der Storage Virtual Machine (SVM) nicht konfiguriert und aktiviert ist.

  Wenn Sie jedoch möchten, dass die Freigabe zwischengespeicherte Inhalte anbietet, müssen Sie BranchCache auf der SVM konfigurieren und aktivieren.

- Da beim Verwenden des `-share-properties` Parameters keine Standard-Freigabeeigenschaften auf die Freigabe angewendet werden, müssen alle anderen Freigabeeigenschaften, die zusätzlich zur `branchcache` Freigabeeigenschaft auf die Freigabe angewendet werden sollen, durch eine durch Kommas getrennte Liste angegeben werden.
- Weitere Informationen zu `vserver cifs share create` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Erstellen Sie eine BranchCache-fähige SMB-Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name <share_name>
-path <path> -share-properties branchcache[,...]
```

2. Überprüfen Sie, ob die BranchCache-Freigabeeigenschaft für die SMB-Freigabe festgelegt ist:

```
vserver cifs share show
```

Beispiel

Der folgende Befehl erstellt eine BranchCache-fähige SMB-Freigabe mit dem Namen „data“ und einem Pfad von `/data` auf SVM vs1. Standardmäßig ist die Einstellung für Offline-Dateien auf `manual` gesetzt:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                     Vserver: vs1
                       Share: data
     CIFS Server NetBIOS Name: VS1
                        Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
```

```
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Verwandte Informationen

Deaktivieren Sie BranchCache für eine einzelne Freigabe

Aktivieren Sie BranchCache auf bestehenden ONTAP SMB-Freigaben

Sie können BranchCache auf einer bestehenden SMB-Freigabe aktivieren, indem Sie die `branchcache` Freigabeeigenschaft zur bestehenden Liste der Freigabeeigenschaften hinzufügen.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Offline-Dateikonfiguration der Freigabe auf manuelles Caching eingestellt sein.

  Wenn die Einstellung für Offline-Dateien der vorhandenen Freigabe nicht auf manuelles Caching gesetzt ist, muss dies durch Ändern der Freigabe konfiguriert werden.

- Sie können die `branchcache`Eigenschaft für eine Freigabe festlegen, selbst wenn BranchCache auf der Storage Virtual Machine (SVM) nicht konfiguriert und aktiviert ist.

  Wenn Sie jedoch möchten, dass die Freigabe zwischengespeicherte Inhalte anbietet, müssen Sie BranchCache auf der SVM konfigurieren und aktivieren.

- Wenn die `branchcache`Freigabeeigenschaft zur Freigabe hinzugefügt wird, bleiben die bestehenden Freigabeeinstellungen und Freigabeeigenschaften erhalten.

  Die BranchCache Share-Eigenschaft wird der bestehenden Liste der Share-Eigenschaften hinzugefügt. Weitere Informationen zu `vserver cifs share properties add` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Gegebenenfalls die Einstellung für die Offline-Dateifreigabe für manuelle Zwischenspeicherung konfigurieren:
   a. Welche Einstellung für die Offline-Dateifreigabe vorliegt, lässt sich mit dem `vserver cifs share show` Befehl feststellen.
   b. Wenn die Einstellung für die Offline-Dateifreigabe nicht auf manuell gesetzt ist, sollte sie auf den erforderlichen Wert geändert werden: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. BranchCache auf einer bestehenden SMB-Freigabe aktivieren: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`

3. Es sollte überprüft werden, ob die BranchCache-Freigabeeigenschaft für die SMB-Freigabe festgelegt ist:
   `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiel

Der folgende Befehl aktiviert BranchCache auf einer bestehenden SMB-Freigabe mit dem Namen “data2” und dem Pfad `/data2` auf SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
```

```
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Verwandte Informationen

- Freigabeeigenschaften bei bestehenden Shares hinzufügen oder entfernen
- Deaktivieren Sie BranchCache für eine einzelne Freigabe

Deaktivieren Sie BranchCache auf SMB-Freigaben

Wenn Sie keine BranchCache-Caching-Dienste für bestimmte SMB-Freigaben bereitstellen möchten, aber möglicherweise später Caching-Dienste auf diesen Freigaben anbieten wollen, kann BranchCache für jede Freigabe einzeln deaktiviert werden. Wenn BranchCache so konfiguriert ist, dass Caching für alle Freigaben angeboten wird, Sie jedoch alle Caching-Dienste vorübergehend deaktivieren möchten, kann die BranchCache-Konfiguration so geändert werden, dass das automatische Caching auf allen Freigaben gestoppt wird.

Wenn BranchCache auf einer SMB-Freigabe nach der ersten Aktivierung anschließend deaktiviert wird, stellt ONTAP das Senden von Metadaten an den anfragenden Client ein. Ein Client, der Daten benötigt, ruft diese direkt vom Content-Server (CIFS-Server auf der Storage Virtual Machine (SVM)) ab.

Deaktivieren von BranchCache auf einer einzelnen ONTAP SMB-Freigabe

Wenn für bestimmte Freigaben, die zuvor zwischengespeicherte Inhalte angeboten haben, keine Caching-Dienste mehr angeboten werden sollen, kann BranchCache auf einer bestehenden SMB-Freigabe deaktiviert werden.

Schritt

1. Führen Sie den folgenden Befehl aus:

   ```
   vserver cifs share properties remove -vserver <SVM_name> -share-name
   <share_name> -share-properties branchcache
   ```

   Die BranchCache Share-Eigenschaft wird entfernt. Andere angewendete Share-Eigenschaften bleiben bestehen.

Beispiel

Der folgende Befehl deaktiviert BranchCache auf einer bestehenden SMB-Freigabe mit dem Namen “data2”:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                    Vserver: vs1
                      Share: data2
    CIFS Server NetBIOS Name: VS1
                       Path: /data2
```

```
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Automatisches Caching für alle ONTAP SMB-Freigaben deaktivieren

Wenn Ihre BranchCache Konfiguration das Caching auf allen SMB-Freigaben auf jeder Storage Virtual Machine (SVM) automatisch aktiviert, kann die BranchCache Konfiguration so angepasst werden, dass das automatische Caching von Inhalten für alle SMB-Freigaben beendet wird.

Über diese Aufgabe

Um das automatische Caching auf allen SMB-Freigaben zu beenden, wird der BranchCache Betriebsmodus auf Caching pro Freigabe geändert.

Schritte

1. Konfigurieren Sie BranchCache, um die automatische Zwischenspeicherung auf allen SMB-Freigaben zu stoppen:

```
vserver cifs branchcache modify -vserver <SVM_name> -operating-mode per-
share
```

2. Überprüfen Sie, ob die BranchCache-Konfiguration korrekt ist:

```
vserver cifs branchcache show -vserver <SVM_name>
```

Beispiel

Der folgende Befehl ändert die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM, früher bekannt als Vserver) vs1, sodass das automatische Caching auf allen SMB-Freigaben gestoppt wird:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Verwandte Informationen

Informationen zur Konfiguration von BranchCache-aktivierten Freigaben

Deaktivieren oder Aktivieren von BranchCache auf einer ONTAP SVM

Wenn Sie zuvor BranchCache konfiguriert haben, aber nicht möchten, dass die Clients der Zweigstelle zwischengespeicherte Inhalte verwenden, können Sie das Caching auf dem CIFS-Server deaktivieren. Sie müssen sich darüber im Klaren sein, was passiert, wenn Sie BranchCache deaktivieren. Sie können BranchCache auf der Storage Virtual Machine deaktivieren, indem Sie den BranchCache-Betriebsmodus auf „Deaktiviert“ ändern. Sie können BranchCache jederzeit wieder aktivieren, indem Sie den Betriebsmodus so ändern, dass entweder BranchCache-Dienste pro Freigabe oder automatisch für alle Freigaben angeboten werden.

Wenn Sie BranchCache deaktivieren, berechnet ONTAP keine Hashes mehr und sendet die Metadaten nicht mehr an den anfordernden Client. Es kommt jedoch zu keiner Unterbrechung des Dateizugriffs. Wenn für BranchCache aktivierte Clients danach Metadateninformationen für Inhalte anfordern, auf die sie zugreifen möchten, antwortet ONTAP mit einem von Microsoft definierten Fehler, was den Client veranlasst, eine zweite

Anforderung zu senden, mit der der tatsächliche Inhalt angefordert wird. Als Antwort auf die Anforderung von Inhalten sendet der CIFS-Server den tatsächlichen Inhalt, der auf der Storage Virtual Machine (SVM) gespeichert ist.

Nachdem BranchCache auf dem CIFS-Server deaktiviert wurde, werben SMB-Freigaben keine BranchCache-Funktionen mehr. Für den Zugriff auf Daten bei neuen SMB-Verbindungen stellen Clients normale SMB-Leseanforderungen.

Die Funktion BranchCache kann auf dem CIFS-Server jederzeit wieder aktiviert werden.

- Da der Hash-Speicher beim Deaktivieren von BranchCache nicht gelöscht wird, kann ONTAP die gespeicherten Hashes verwenden, wenn nach dem erneuten Aktivieren von BranchCache auf Hash-Anfragen geantwortet wird, vorausgesetzt, der angeforderte Hash ist noch gültig.
- Clients, die während der Deaktivierung von BranchCache SMB-Verbindungen zu BranchCache-fähigen Freigaben hergestellt haben, erhalten keinen BranchCache-Support, wenn BranchCache anschließend wieder aktiviert wird.

  Dies liegt daran, dass ONTAP die BranchCache-Unterstützung für eine Freigabe zum Zeitpunkt des SMB-Sitzungsaufbaus signalisiert. Clients, die Sitzungen zu BranchCache-aktivierten Freigaben hergestellt haben, während BranchCache deaktiviert war, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.

> Wenn Sie den Hash-Speicher nach der Deaktivierung von BranchCache auf einem CIFS-Server nicht speichern möchten, kann er manuell gelöscht werden. Wenn BranchCache erneut aktiviert wird, muss sichergestellt sein, dass das Hash-Speicherverzeichnis vorhanden ist. Nach der erneuten Aktivierung von BranchCache geben BranchCache-aktivierte Freigaben BranchCache-Funktionen bekannt. ONTAP erstellt neue Hashes, wenn neue Anfragen von BranchCache-aktivierten Clients gestellt werden.

Schritte

1. Führen Sie den entsprechenden Befehl aus:

Wenn Sie möchten…	Geben Sie anschließend Folgendes ein…
BranchCache deaktivieren	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Aktivieren Sie BranchCache pro Freigabe	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
Aktivieren Sie BranchCache für alle Freigaben	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Es sollte überprüft werden, ob der BranchCache Betriebsmodus mit der gewünschten Einstellung konfiguriert ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Das folgende Beispiel deaktiviert BranchCache auf SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
```

```
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Die BranchCache Konfiguration auf ONTAP SMB-Freigaben löschen

Wenn Sie zuvor BranchCache konfiguriert haben, aber nicht möchten, dass die Storage Virtual Machine (SVM) weiterhin zwischengespeicherte Inhalte bereitstellt, kann die BranchCache-Konfiguration auf dem CIFS-Server gelöscht werden. Es muss beachtet werden, was beim Löschen der Konfiguration geschieht.

Wenn die Konfiguration gelöscht wird, entfernt ONTAP die Konfigurationsinformationen für diese SVM aus dem Cluster und stoppt den BranchCache-Dienst. Es kann ausgewählt werden, ob ONTAP den Hash-Speicher auf der SVM löschen soll.

Das Löschen der BranchCache-Konfiguration unterbricht nicht den Zugriff durch BranchCache-fähige Clients. Wenn BranchCache-fähige Clients danach Metadateninformationen zu bestehenden SMB-Verbindungen für bereits im Cache gespeicherte Inhalte anfordern, antwortet ONTAP mit einem von Microsoft definierten Fehler, was den Client veranlasst, eine zweite Anfrage zu senden, mit der der tatsächliche Inhalt angefordert wird. Als Antwort auf die Anfrage nach Inhalten sendet der CIFS-Server den tatsächlichen Inhalt, der auf der SVM gespeichert ist

Nach dem Löschen der BranchCache-Konfiguration geben die SMB-Freigaben keine BranchCache-Funktionen mehr bekannt. Um auf Inhalte zuzugreifen, die zuvor nicht zwischengespeichert wurden, stellen Clients über neue SMB-Verbindungen normale SMB-Leseanforderungen.

Der Befehl, den Sie zum Löschen des BranchCache-Dienstes auf Ihrer Storage Virtual Machine (SVM) verwenden, unterscheidet sich je nachdem, ob vorhandene Hashes gelöscht oder beibehalten werden sollen.

Schritt

1. Führen Sie den entsprechenden Befehl aus:

Wenn Sie möchten…	Geben Sie anschließend Folgendes ein…
Die BranchCache Konfiguration und die vorhandenen Hashes löschen	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Die BranchCache Konfiguration löschen, aber vorhandene Hashes beibehalten	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Beispiel

Das folgende Beispiel löscht die BranchCache Konfiguration auf SVM vs1 und löscht alle vorhandenen

Hashes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Die BranchCache Konfiguration verwalten und überwachen

Konfigurationen von BranchCache auf ONTAP SMB-Freigaben anpassen

Sie können die Konfiguration des BranchCache-Dienstes auf SVMs anpassen, einschließlich der Änderung des Pfads zum Hash-Speicherverzeichnis, der maximalen Größe des Hash-Speicherverzeichnisses, des Betriebsmodus und der unterstützten BranchCache-Versionen. Auch die Größe des Volumes, das den Hash-Speicher enthält, kann erhöht werden.

Schritte

1. Die entsprechende Maßnahme ausführen:

Wenn Sie möchten…	Geben Sie Folgendes ein…
Die Größe des Hash-Speicherverzeichnisses anpassen	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Die Größe des Volumes, das den Hash-Speicher enthält, erhöhen	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]`Wenn das Volume, das den Hash-Speicher enthält, voll ist, kann möglicherweise die Größe des Volumes erhöht werden. Die neue Volume-Größe kann als Zahl gefolgt von einer Einheit angegeben werden. Erfahren Sie mehr über"Verwaltung von FlexVol-Volumes"	Den Pfad des Hash-Speicherverzeichnisses ändern

Wenn Sie möchten…	Geben Sie Folgendes ein…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}`Wenn die SVM eine SVM-Disaster-Recovery-Quelle ist, darf sich der Hash-Pfad nicht auf dem Root-Volume befinden. Dies liegt daran, dass das Root Volume nicht auf das Notfallwiederherstellungsziel repliziert wird. Der BranchCache Hash-Pfad kann Leerzeichen und beliebige gültige Dateinamenzeichen enthalten. Wenn Sie den Hash-Pfad ändern, ist `-flush -hashes` ein erforderlicher Parameter, der angibt, ob ONTAP die Hashes aus dem ursprünglichen Hash-Speicherort löschen soll. Für den `-flush -hashes` Parameter können die folgenden Werte festgelegt werden: **Wenn `true` angegeben wird, löscht ONTAP die Hashes am ursprünglichen Speicherort und erstellt neue Hashes am neuen Speicherort, sobald neue Anfragen von BranchCache-fähigen Clients eingehen.** Wenn `false` angegeben wird, werden die Hashes nicht gelöscht. + In diesem Fall kann die vorhandenen Hashes später wiederverwendet werden, indem der Pfad zum Hash-Speicher wieder auf den ursprünglichen Speicherort geändert wird.
Den Betriebsmodus ändern	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Beim Ändern des Betriebsmodus ist Folgendes zu beachten: **ONTAP signalisiert BranchCache-Unterstützung für eine Freigabe, wenn die SMB-Sitzung eingerichtet wird.** Clients, die bereits Sitzungen aufgebaut haben, wenn BranchCache aktiviert wird, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe nutzen zu können.
Die Unterstützung der BranchCache Version ändern	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Die Konfigurationsänderungen lassen sich mit dem `vserver cifs branchcache show` Befehl überprüfen.

Informationen zu BranchCache Konfigurationen auf ONTAP SMB-Freigaben

Informationen zu BranchCache Konfigurationen auf Storage Virtual Machines (SVMs) können angezeigt werden, was bei der Überprüfung einer Konfiguration oder bei der Ermittlung der aktuellen Einstellungen vor einer Änderung der Konfiguration hilfreich ist.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie anzeigen möchten…	Geben Sie diesen Befehl ein…
Zusammenfassende Informationen zu BranchCache Konfigurationen auf allen SVMs	`vserver cifs branchcache show`
Detaillierte Informationen zur Konfiguration einer bestimmten SVM	`vserver cifs branchcache show -vserver` *`vserver_name`*

Beispiel

Das folgende Beispiel zeigt Informationen zur BranchCache Konfiguration auf SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
            Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

Den ONTAP SMB BranchCache Server-Schlüssel ändern

Sie können den BranchCache Server-Schlüssel ändern, indem Sie die BranchCache Konfiguration auf der Storage Virtual Machine (SVM) modifizieren und einen anderen Server-Schlüssel angeben.

Über diese Aufgabe

Sie können den Serverschlüssel auf einen bestimmten Wert setzen, sodass, falls mehrere Server BranchCache-Daten für dieselben Dateien bereitstellen, Clients Hashes von jedem Server mit demselben Serverschlüssel verwenden können.

Wenn Sie den Serverschlüssel ändern, müssen Sie auch den Hash-Cache leeren. Nach dem Leeren der Hashes erstellt ONTAP neue Hashes, sobald neue Anfragen von BranchCache-aktivierten Clients gestellt werden.

Schritte

1. Der Serverschlüssel kann mit folgendem Befehl geändert werden: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   Bei der Konfiguration eines neuen Serverschlüssels müssen auch `-flush-hashes` angegeben und der Wert auf `true` gesetzt werden.

2. Es kann überprüft werden, ob die BranchCache Konfiguration korrekt ist, indem der `vserver cifs branchcache show` Befehl verwendet wird.

Beispiel

Das folgende Beispiel legt einen neuen Serverschlüssel fest, der Leerzeichen enthält, und leert den Hash-Cache auf SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Verwandte Informationen

Informationen zu den Gründen, aus denen ONTAP BranchCache-Hashes für ungültig erklärt

Vorkalkulation von BranchCache-Hashes auf angegebenen ONTAP SMB-Pfaden

Sie können den BranchCache Service so konfigurieren, dass Hashwerte für eine einzelne Datei, ein Verzeichnis oder alle Dateien in einer Verzeichnisstruktur vorab berechnet werden. Dies kann hilfreich sein, wenn Hashwerte für Daten in einer BranchCache-fähigen Freigabe außerhalb der Spitzenzeiten berechnet werden sollen.

Über diese Aufgabe

Wenn Sie vor der Anzeige der Hash-Statistiken eine Datenprobe erfassen möchten, müssen Sie die `statistics start` und optionalen `statistics stop` Befehle verwenden.

- Es ist erforderlich, die Storage Virtual Machine (SVM) und den Pfad anzugeben, auf dem Hashes vorab berechnet werden sollen.
- Es muss außerdem angegeben werden, ob die Hashwerte rekursiv berechnet werden sollen.
- Wenn Sie Hashes rekursiv berechnen möchten, durchläuft der BranchCache-Dienst den gesamten Verzeichnisbaum unter dem angegebenen Pfad und berechnet Hashes für jedes geeignete Objekt.

  Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Hashwerte nach Bedarf vorab berechnen:

Wenn Sie Hashwerte vorab berechnen möchten…	Geben Sie den Befehl ein…
Eine einzelne Datei oder ein Verzeichnis	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Rekursiv auf alle Dateien in einer Verzeichnisstruktur	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Es kann mit dem `statistics` Befehl überprüft werden, ob Hashwerte berechnet werden:

   a. Statistiken für das `hashd` Objekt auf der gewünschten SVM-Instanz anzeigen: `statistics show -object hashd -instance vserver_name`

   b. Es kann überprüft werden, ob die Anzahl der erzeugten Hashes durch Wiederholung des Befehls zunimmt.

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

Beispiele

Das folgende Beispiel erzeugt Hashes für den Pfad `/data` und alle darin enthaltenen Dateien und Unterverzeichnisse auf SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
```

```
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Verwandte Informationen

- "Einrichtung der Leistungsüberwachung"

Hashes aus dem ONTAP SMB SVM BranchCache Hash-Speicher löschen

Sie können alle zwischengespeicherten Hashes aus dem BranchCache Hash-Speicher auf der Storage Virtual Machine (SVM) löschen. Dies kann hilfreich sein, wenn die BranchCache Konfiguration der Zweigstelle geändert wurde. Wenn beispielsweise der Caching-Modus kürzlich von verteiltem Caching auf gehosteten Caching-Modus umgestellt wurde, empfiehlt sich das Leeren des Hash-Speichers.

Über diese Aufgabe

Nach dem Leeren der Hashes erstellt ONTAP neue Hashes, sobald neue Anfragen von BranchCache-aktivierten Clients gestellt werden.

Schritt

1. Die Hashes aus dem BranchCache Hash-Speicher werden entfernt: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

ONTAP SMB BranchCache Statistiken anzeigen

Sie können BranchCache Statistiken anzeigen, um unter anderem festzustellen, wie gut das Caching funktioniert, ob Ihre Konfiguration zwischengespeicherte Inhalte für Clients bereitstellt und ob Hash-Dateien gelöscht wurden, um Platz für aktuellere Hash-Daten zu schaffen.

Über diese Aufgabe

Das `hashd` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-Hashwerte liefern. Das `cifs` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-bezogene Aktivitäten liefern. Informationen über diese Objekte können auf der erweiterten Berechtigungsebene gesammelt und angezeigt werden.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. Die BranchCache-bezogenen Zähler werden mit dem `statistics catalog counter show` Befehl angezeigt.

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    --------------------------
---------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.
```

```
cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                      Description
    ---------------------------
-----------------------------------------------
    active_searches              Number of active searches over SMB and
SMB2
    auth_reject_too_many         Authentication refused after too many
                                 requests were made in rapid succession
    avg_directory_depth          Average number of directories crossed by
SMB
                                 and SMB2 path-based commands
    avg_junction_depth           Average number of junctions crossed by
SMB
                                 and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                 data failed. These are failures when
                                 attempting to read existing hash data.
It
                                 does not include attempts to fetch hash
data
                                 that has not yet been generated.
    branchcache_hash_fetch_ok    Total number of times a request to fetch
hash
                                 data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                 requesting hashes.
    branchcache_missing_hash_bytes
                                 Total number of bytes of data that had
to be
                                 read by the client because the hash for
that
                                 content was not available on the server.
   ....Output truncated....
```

Weitere Informationen zu `statistics catalog counter show` finden sich in der "ONTAP-Befehlsreferenz".

3. Mit den `statistics start`- und `statistics stop`-Befehlen lassen sich BranchCache-bezogene Statistiken erfassen.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11
```

```
cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

4. Die gesammelten BranchCache-Statistiken werden mit dem `statistics show` Befehl angezeigt.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                    0
    branchcache_hash_sent_bytes                                    0
    branchcache_hash_sent_bytes                                    0
    branchcache_hash_sent_bytes                                    0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                 0
    branchcache_missing_hash_bytes                                 0
    branchcache_missing_hash_bytes                                 0
    branchcache_missing_hash_bytes                                 0
```

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

5. Zurück zur Administratorrechteebene: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Verwandte Informationen

- Statistiken anzeigen
- "Einrichtung der Leistungsüberwachung"
- "Statistiken Start"
- "Statistiken stoppen"

Informationen zur ONTAP SMB-Unterstützung für BranchCache Gruppenrichtlinienobjekte

ONTAP BranchCache bietet Unterstützung für BranchCache Gruppenrichtlinienobjekte (GPOs), die eine zentrale Verwaltung bestimmter BranchCache Konfigurationsparameter ermöglichen. Es gibt zwei GPOs, die für BranchCache verwendet werden: die Hash Publication for BranchCache GPO und die Hash Version Support for BranchCache GPO.

- **Hash-Veröffentlichung für BranchCache GPO**

  Die Hash-Veröffentlichung für BranchCache GPO entspricht dem `-operating-mode` Parameter. Bei GPO-Aktualisierungen wird dieser Wert auf Storage Virtual Machine (SVM)-Objekte angewendet, die sich in der Organisationseinheit (OU) befinden, auf die die Gruppenrichtlinie zutrifft.

- **Unterstützung von Hash-Versionen für BranchCache GPO**

  Die Hash-Versionsunterstützung für BranchCache GPO entspricht dem `-versions` Parameter. Bei GPO-Aktualisierungen wird dieser Wert auf SVM-Objekte angewendet, die sich in der Organisationseinheit befinden, auf die die Gruppenrichtlinie angewendet wird.

Verwandte Informationen

Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server

Informationen zu ONTAP SMB BranchCache Gruppenrichtlinienobjekten

Es lassen sich Informationen zur Gruppenrichtlinienobjekt-(GPO-)Konfiguration des CIFS-Servers anzeigen, um zu ermitteln, ob BranchCache-GPOs für die Domäne, zu der der CIFS-Server gehört, definiert sind und, falls ja, welche Einstellungen zulässig sind. Es lässt sich außerdem feststellen, ob BranchCache-GPO-Einstellungen auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Auch wenn eine Gruppenrichtlinieneinstellung (GPO) in der Domäne definiert ist, zu der der CIFS-Server gehört, wird sie nicht zwangsläufig auf die Organisationseinheit (OU) angewendet, die die CIFS-fähige Storage Virtual Machine (SVM) enthält. Angewendete GPO-Einstellungen sind die Teilmenge aller definierten GPOs, die auf die CIFS-fähige SVM angewendet werden. BranchCache-Einstellungen, die über GPOs angewendet werden, überschreiben Einstellungen, die über die CLI angewendet werden.

Schritte

1. Die definierte BranchCache-Gruppenrichtlinieneinstellung für die Active Directory-Domäne wird mit dem `vserver cifs group-policy show-defined` Befehl angezeigt.

Dieses Beispiel zeigt nicht alle verfügbaren Ausgabefelder des Befehls an. Die Ausgabe ist gekürzt.

```
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
  [...]

    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
  [...]
```

2. Die BranchCache-Gruppenrichtlinie, die auf den CIFS-Server angewendet wurde, wird mit dem `vserver cifs group-policy show-applied` Befehl angezeigt. ``

Dieses Beispiel zeigt nicht alle verfügbaren Ausgabefelder des Befehls an. Die Ausgabe ist gekürzt.

```
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: version1
  [...]

    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: version1
 [...]
```

Verwandte Informationen

- GPO-Unterstützung auf Servern aktivieren oder deaktivieren
- "vserver cifs group-policy show-defined"
- "vserver cifs group-policy show-applied"

Was mit ONTAP SMB BranchCache beim Zurücksetzen geschieht

Es ist wichtig zu verstehen, was passiert, wenn ONTAP auf eine Version zurückgesetzt wird, die BranchCache nicht unterstützt.

- Wenn auf eine Version von ONTAP zurückgegangen wird, die BranchCache nicht unterstützt, geben die SMB-Freigaben keine BranchCache-Funktionen an BranchCache-fähige Clients bekannt; daher fordern die Clients keine Hash-Informationen an.

  Stattdessen fordern sie die eigentlichen Inhalte über normale SMB-Leseanfragen an. Als Antwort auf die Anforderung von Inhalten sendet der SMB-Server den tatsächlichen Inhalt, der auf der Storage Virtual Machine (SVM) gespeichert ist.

- Wenn ein Knoten, der einen Hash-Speicher hostet, auf eine Version zurückgesetzt wird, die BranchCache nicht unterstützt, muss der Speicheradministrator die BranchCache-Konfiguration manuell mit einem Befehl zurücksetzen, der während des Rücksetzungsvorgangs ausgegeben wird.

  Dieser Befehl löscht die BranchCache Konfiguration und Hashes.

  Nach Abschluss des Revert-Vorgangs kann der Storage-Administrator das Verzeichnis, das den Hash Store enthielt, bei Bedarf manuell löschen.

Verwandte Informationen

Die BranchCache Konfiguration auf Freigaben löschen

Verbesserung der Microsoft Remote Copy Leistung

Informationen zu Leistungsverbesserungen von Microsoft Remote Copy auf ONTAP SMB-Servern

Microsoft Offloaded Data Transfer (ODX), auch bekannt als Copy Offload, ermöglicht direkte Datenübertragungen innerhalb oder zwischen kompatiblen Speichermedien, ohne dass die Daten über den Host-Computer übertragen werden.

ONTAP unterstützt ODX sowohl für das SMB- als auch für das SAN-Protokoll. Die Quelle kann entweder ein CIFS-Server oder eine LUN sein, und das Ziel kann ebenfalls ein CIFS-Server oder eine LUN sein.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk zum Client-Computer übertragen. Der Client-Computer überträgt die Daten dann über das Netzwerk zurück zum Ziel. Zusammengefasst liest der Client-Computer die Daten von der Quelle und schreibt sie zum Ziel. Bei ODX-Dateiübertragungen werden die Daten direkt von der Quelle zum Ziel kopiert.

Da ODX-Offloaded-Kopien direkt zwischen Quell- und Zielspeicher durchgeführt werden, ergeben sich erhebliche Leistungsvorteile. Zu den realisierten Leistungsvorteilen zählen eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client sowie eine reduzierte Auslastung der Netzwerk-I/O-Bandbreite.

In SMB-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Speicherserver SMB 3.0 und die ODX-Funktion unterstützen. In SAN-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Speicherserver die ODX-Funktion unterstützen. Clientcomputer, die ODX unterstützen und bei denen ODX aktiviert ist, nutzen beim Verschieben oder Kopieren von Dateien automatisch und transparent die ausgelagerte Dateiübertragung. ODX wird unabhängig davon verwendet, ob Dateien per Drag-and-Drop im Windows Explorer verschoben werden, Befehlszeilenbefehle zum Kopieren genutzt werden oder ob eine Clientanwendung Dateikopieranforderungen initiiert.

Verwandte Informationen

- Informationen zur Verbesserung der Client-Reaktionszeit durch automatische Knotenverweise mit Auto Location
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"

Informationen zu ODX auf ONTAP SMB-Servern

ODX Copy Offload verwendet einen tokenbasierten Mechanismus zum Lesen und Schreiben von Daten innerhalb oder zwischen ODX-fähigen CIFS-Servern. Anstatt die Daten über den Host zu leiten, sendet der CIFS-Server ein kleines Token, das die Daten repräsentiert, an den Client. Der ODX-Client präsentiert dieses Token dem Zielserver, der dann die durch das Token repräsentierten Daten vom Quell- zum Zielserver übertragen kann.

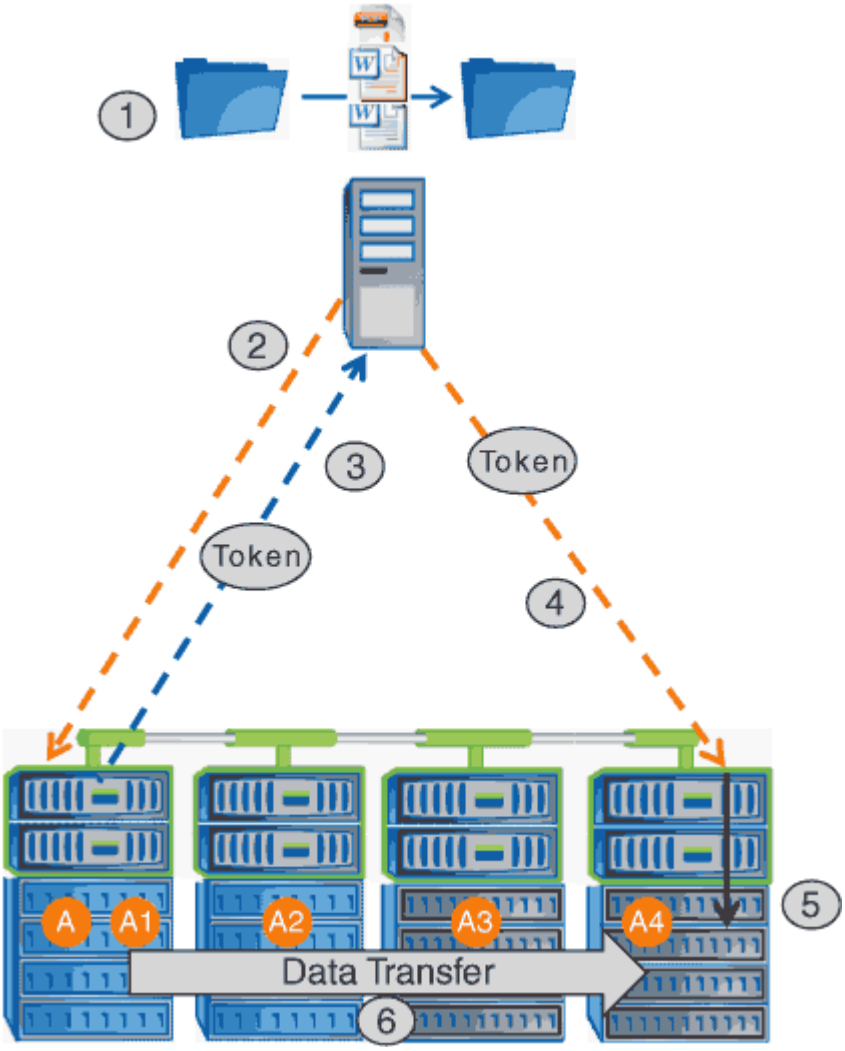
Sobald ein ODX-Client feststellt, dass der CIFS-Server ODX-fähig ist, öffnet er die Quelldatei und fordert ein Token vom CIFS-Server an. Nach dem Öffnen der Zieldatei verwendet der Client das Token, um den Server anzuweisen, die Daten direkt von der Quelle zur Zieldatei zu kopieren.

Quelle und Ziel können sich auf derselben Storage Virtual Machine (SVM) oder auf verschiedenen SVMs befinden, abhängig vom Umfang des Kopiervorgangs.

Das Token dient als zeitpunktgenaue Darstellung der Daten. Beispielsweise wird beim Kopieren von Daten zwischen Speicherorten ein Token, das ein Datensegment repräsentiert, an den anfragenden Client zurückgegeben, welches der Client an das Ziel kopiert, sodass das Kopieren der zugrundeliegenden Daten über den Client entfällt.

ONTAP unterstützt Tokens, die jeweils 8 MB Daten repräsentieren. ODX Kopien von mehr als 8 MB werden mithilfe mehrerer Tokens durchgeführt, wobei jedes Token 8 MB Daten repräsentiert.

Die folgende Abbildung erläutert die Schritte, die bei einem ODX Kopiervorgang anfallen:



1. Ein Benutzer kopiert oder verschiebt eine Datei mithilfe von Windows Explorer, einer Befehlszeilenschnittstelle oder im Rahmen einer Migration einer virtuellen Maschine, oder eine Anwendung initiiert Dateikopien oder -verschiebungen.
2. Der ODX-fähige Client übersetzt diese Übertragungsanforderung automatisch in eine ODX-Anforderung.

   Die ODX-Anfrage, die an den CIFS-Server gesendet wird, enthält eine Anfrage für ein Token.

3. Wenn ODX auf dem CIFS-Server aktiviert ist und die Verbindung über SMB 3.0 erfolgt, generiert der CIFS-Server ein Token, das eine logische Repräsentation der Daten auf der Quelle darstellt.

4. Der Client empfängt ein Token, das die Daten repräsentiert, und sendet es zusammen mit der Schreibanforderung an den Ziel-CIFS-Server.

   Dies sind die einzigen Daten, die über das Netzwerk von der Quelle zum Client und dann vom Client zum Ziel kopiert werden.

5. Das Token wird an das Speichersubsystem übermittelt.
6. Die SVM führt das Kopieren oder Verschieben intern durch.

   Ist die zu kopierende oder zu verschiebende Datei größer als 8 MB, werden mehrere Tokens benötigt, um den Kopiervorgang durchzuführen. Die Schritte 2 bis 6 werden nach Bedarf ausgeführt, um den Kopiervorgang abzuschließen.

> Wenn beim ODX-basierten Auslagern des Kopiervorgangs ein Fehler auftritt, wird für den Kopier- oder Verschiebevorgang auf herkömmliche Lese- und Schreibvorgänge zurückgegriffen. Ebenso wird für den Kopier- oder Verschiebevorgang auf herkömmliche Lese- und Schreibvorgänge zurückgegriffen, wenn der Ziel-CIFS-Server ODX nicht unterstützt oder ODX deaktiviert ist.

Anforderungen für die Verwendung von ODX auf ONTAP SMB-Servern

Bevor Sie ODX für Copy Offloads mit Ihrer Storage Virtual Machine (SVM) verwenden können, sind bestimmte Voraussetzungen zu berücksichtigen.

ONTAP Versionsanforderungen

ONTAP Releases unterstützen ODX für Copy-Offloads.

SMB Versionsanforderungen

- ONTAP unterstützt ODX mit SMB 3.0 und höher.
- SMB 3.0 muss auf dem CIFS-Server aktiviert sein, bevor ODX aktiviert werden kann:
  - Durch die Aktivierung von ODX wird auch SMB 3.0 aktiviert, falls es nicht bereits aktiviert ist.
  - Durch das Deaktivieren von SMB 3.0 wird auch ODX deaktiviert.

Anforderungen an Windows Server und Client

Bevor Sie ODX für Copy-Offloads verwenden können, muss der Windows Client diese Funktion unterstützen.

Die "NetApp Interoperabilitätsmatrix"enthält die neuesten Informationen zu unterstützten Windows-Clients.

Volumenanforderungen

- Die Quellvolumes müssen mindestens 1,25 GB groß sein.
- Bei Verwendung komprimierter Volumes muss der Komprimierungstyp adaptiv sein und es wird nur die Komprimierungsgruppengröße 8K unterstützt.

  Sekundärer Kompressionstyp wird nicht unterstützt.

Richtlinien für die Verwendung von ODX auf ONTAP SMB Servern

Bevor Sie ODX für Copy-Offload verwenden können, müssen Sie die Richtlinien kennen. Beispielsweise müssen Sie wissen, auf welchen Volume-Typen Sie ODX verwenden können, und die Überlegungen zu ODX innerhalb und zwischen Clustern verstehen.

Volumenrichtlinien

- ODX kann für Copy Offload bei folgenden Volume-Konfigurationen nicht verwendet werden:
  - Die Größe des Quellvolumes beträgt weniger als 1,25 GB

    Die Volume-Größe muss mindestens 1,25 GB betragen, um ODX zu verwenden.
  - Schreibgeschützte Volumes

    ODX wird nicht für Dateien und Ordner verwendet, die sich auf Load-Sharing-Mirrors oder in SnapMirror oder SnapVault Zielvolumes befinden.
  - Wenn das Quellvolume nicht dedupliziert ist
- ODX-Kopien werden nur für Intra-Cluster-Kopien unterstützt.

  Mit ODX ist das Kopieren von Dateien oder Ordnern auf ein Volume in einem anderen Cluster nicht möglich.

Weitere Richtlinien

- In SMB-Umgebungen müssen die Dateien mindestens 256 KB groß sein, damit ODX für Copy-Offload verwendet werden kann.

  Kleinere Dateien werden mittels eines herkömmlichen Kopiervorgangs übertragen.
- ODX Copy Offload nutzt Deduplizierung als Teil des Kopiervorgangs.

  Wenn keine Deduplizierung auf SVM-Volumes beim Kopieren oder Verschieben von Daten erfolgen soll, ist ODX Copy Offload auf diesem SVM zu deaktivieren.
- Die Anwendung, die den Datentransfer durchführt, muss so geschrieben sein, dass sie ODX unterstützt.

  Zu den Anwendungsoperationen, die ODX unterstützen, gehören die folgenden:
  - Hyper-V Managementvorgänge, wie das Erstellen und Konvertieren virtueller Festplatten (VHDs), das Verwalten von Snapshots und das Kopieren von Dateien zwischen virtuellen Maschinen

    ODX Copy Offload Pass-Through unterstützt Kopiervorgänge, die von einem Hyper-V-Gastbetriebssystem initiiert werden. Das Gastbetriebssystem muss ODX unterstützen und SCSI-Virtual-Disks verwenden, die von ODX-fähigem SMB- oder SAN-Speicher unterstützt werden. IDE-Virtual-Disks unterstützen ODX Pass-Through nicht. Quell- und Zielspeicher müssen sich im selben Cluster befinden.

    Weitere Informationen finden sich unter "Anwendungsfälle für ODX auf ONTAP SMB Servern".
  - Windows Explorer Operationen
  - Windows PowerShell Kopierbefehle

- Windows-Eingabeaufforderung Kopierbefehle

  Robocopy an der Windows-Eingabeaufforderung unterstützt ODX.

  > Die Anwendungen müssen auf Windows Servern oder Clients ausgeführt werden, die ODX unterstützen.

  +
  Weitere Informationen zu unterstützten ODX-Anwendungen auf Windows Servern und Clients bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anwendungsfälle für ODX auf ONTAP SMB Servern

Sie sollten sich der Anwendungsfälle für die Nutzung von ODX auf SVMs bewusst sein, damit Sie bestimmen können, unter welchen Umständen ODX Ihnen Leistungsvorteile bietet.

Windows Server und Clients, die ODX unterstützen, verwenden Copy Offload als Standardmethode zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows Server oder Client ODX nicht unterstützt oder der ODX Copy Offload an irgendeiner Stelle fehlschlägt, erfolgt der Kopier- oder Verschiebevorgang über herkömmliche Lese- und Schreibvorgänge.

Die folgenden Anwendungsfälle unterstützen die Verwendung von ODX Kopien und ODX Verschiebungen:

- Intra-Volume

  Die Quell- und Zieldateien bzw. LUNs befinden sich im selben Volume.

- Inter-Volume, gleicher Node, gleiche SVM

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf demselben Knoten befinden. Die Daten gehören demselben SVM.

- Inter-Volume, unterschiedliche Knoten, gleiche SVM

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören demselben SVM.

- Inter-SVM, gleicher Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf demselben Knoten befinden. Die Daten gehören verschiedenen SVMs.

- Inter-SVM, verschiedene Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören verschiedenen SVMs.

- Intercluster

  Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten in unterschiedlichen Clustern befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für CIFS.

Es gibt noch einige weitere spezielle Anwendungsfälle:

- Mit der ONTAP ODX Implementierung kann ODX verwendet werden, um Dateien zwischen SMB-Freigaben und an FC oder iSCSI angeschlossenen virtuellen Laufwerken zu kopieren.

  Sie können den Windows Explorer, die Windows CLI oder PowerShell, Hyper-V oder andere Anwendungen, die ODX unterstützen, verwenden, um Dateien nahtlos mithilfe von ODX Copy Offload zwischen SMB-Freigaben und verbundenen LUNs zu kopieren oder zu verschieben, vorausgesetzt, die SMB-Freigaben und LUNs befinden sich im selben Cluster.

- Hyper-V bietet einige zusätzliche Anwendungsfälle für ODX Copy Offload:

  - Mit ODX Copy Offload Pass-Through kann in Verbindung mit Hyper-V Daten innerhalb oder zwischen virtuellen Festplattendateien (VHD) kopiert werden oder Daten zwischen zugeordneten SMB-Freigaben und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

    Dadurch können Kopien von Gastbetriebssystemen an den zugrunde liegenden Speicher weitergegeben werden.

  - Bei der Erstellung von VHDs mit fester Größe wird ODX verwendet, um die Festplatte mit Nullen zu initialisieren, wobei ein bekanntes Null-Token zum Einsatz kommt.
  - ODX Copy Offload wird für die Migration von virtuellen Maschinen-Speichern verwendet, wenn sich Quell- und Zielspeicher im selben Cluster befinden.

> Um die Anwendungsfälle für ODX Copy Offload Pass-Through mit Hyper-V zu nutzen, muss das Gastbetriebssystem ODX unterstützen und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die von einem Speicher (entweder SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten im Gastbetriebssystem unterstützen kein ODX Pass-Through.

ODX auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können ODX auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Standardmäßig ist die Unterstützung für ODX Copy Offload aktiviert, wenn auch SMB 3.0 aktiviert ist.

Bevor Sie beginnen

SMB 3.0 muss aktiviert sein.

Über diese Aufgabe

Wenn Sie SMB 3.0 deaktivieren, deaktiviert ONTAP auch SMB ODX. Wenn Sie SMB 3.0 wieder aktivieren, muss SMB ODX manuell wieder aktiviert werden.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn ODX Copy Offload gewünscht wird…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`

Wenn ODX Copy Offload gewünscht wird…	Geben Sie den Befehl ein…
Deaktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Beispiel

Das folgende Beispiel aktiviert ODX Copy Offload auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

Verfügbare Serveroptionen

Die Client-Antwortzeit wird durch die Bereitstellung von SMB automatischen Knotenverweisen mit Auto Location verbessert.

Informationen zur Verbesserung der Client-Reaktionszeit durch Bereitstellung von ONTAP SMB automatischen Knotenverweisen mit Auto Location

Auto Location nutzt automatische Knotenverweise von SMB, um die Leistung von SMB-Clients auf Storage Virtual Machines (SVMs) zu steigern. Automatische Knotenverweise leiten den anfragenden Client automatisch an eine LIF auf der Node-SVM weiter, die das Volume hostet, in dem sich die Daten befinden, was zu verbesserten Client-Antwortzeiten führen kann.

Wenn ein SMB-Client eine Verbindung zu einer auf der SVM gehosteten SMB-Freigabe herstellt, kann die Verbindung über eine LIF erfolgen, die sich auf einem Knoten befindet, dem die angeforderten Daten nicht gehören. Der Knoten, mit dem der Client verbunden ist, greift über das Clusternetzwerk auf Daten eines anderen Knotens zu. Der Client kann schnellere Antwortzeiten erzielen, wenn die SMB-Verbindung eine LIF auf dem Knoten verwendet, der die angeforderten Daten enthält.

- ONTAP stellt diese Funktionalität bereit, indem Microsoft DFS-Verweise verwendet werden, um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein Ordner im Namespace an einem anderen Ort gehostet wird.

  Ein Knoten führt eine Weiterleitung durch, wenn er feststellt, dass sich auf dem Knoten, der die Daten enthält, ein SVM LIF befindet.

- Automatische Knotenweiterleitungen werden für IPv4- und IPv6-LIF-IP-Adressen unterstützt.
- Weiterleitungen erfolgen auf Grundlage des Speicherorts des Stammverzeichnisses der Freigabe, über die der Client verbunden ist.
- Die Weiterleitung erfolgt während der SMB-Aushandlung.

  Die Weiterleitung erfolgt vor dem Verbindungsaufbau. Nachdem ONTAP den SMB-Client an den Zielknoten weitergeleitet hat, wird die Verbindung hergestellt und der Client greift ab diesem Zeitpunkt über den weitergeleiteten LIF-Pfad auf die Daten zu. Dies ermöglicht den Clients einen schnelleren Zugriff auf die Daten und vermeidet zusätzliche Cluster-Kommunikation.

> Wenn sich eine Freigabe über mehrere Verbindungspunkte erstreckt und einige der Verbindungen auf Volumes auf anderen Knoten liegen, sind die Daten innerhalb der Freigabe auf mehrere Knoten verteilt. Da ONTAP Verweise bereitstellt, die lokal zum Stamm der Freigabe sind, muss ONTAP das Cluster-Netzwerk verwenden, um die Daten in diesen nicht-lokalen Volumes abzurufen. Bei dieser Art von Namespace-Architektur bieten automatische Knotenverweise möglicherweise keine signifikanten Leistungsvorteile.

Verfügt der Knoten, auf dem die Daten gehostet werden, über keine verfügbare LIF, stellt ONTAP die Verbindung über die vom Client gewählte LIF her. Nachdem eine Datei von einem SMB-Client geöffnet wurde, erfolgt der Zugriff weiterhin über dieselbe verwiesene Verbindung.

Kann der CIFS-Server aus irgendeinem Grund keine Weiterleitung vornehmen, kommt es zu keiner Unterbrechung des SMB-Dienstes. Die SMB-Verbindung wird so hergestellt, als wären automatische Knoten-Weiterleitungen nicht aktiviert.

Verwandte Informationen

Verbesserung der Leistung von Microsoft Remote Copy

Anforderungen und Richtlinien für die Verwendung automatischer Knotenverweise auf ONTAP SMB-Servern

Bevor Sie die automatische Knotenweiterleitung in SMB, auch bekannt als *autolocation*, nutzen können, müssen Sie sich bestimmter Anforderungen bewusst sein, einschließlich der ONTAP Versionen, die diese Funktion unterstützen. Sie müssen außerdem über die unterstützten SMB Protokollversionen und bestimmte weitere spezielle Richtlinien informiert sein.

ONTAP Versions- und Lizenzanforderungen

- Alle Knoten im Cluster müssen eine Version von ONTAP ausführen, die automatische Knotenverweise unterstützt.
- Widelinks muss auf einer SMB-Freigabe aktiviert sein, um die Autolokalisierung zu verwenden.
- CIFS muss lizenziert sein, und ein SMB-Server muss auf den SVMs vorhanden 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.

Anforderungen an die SMB-Protokollversion

- Für SVMs unterstützt ONTAP automatische Knotenverweise auf allen Versionen von SMB.

SMB-Client-Anforderungen

Alle von ONTAP unterstützten Microsoft-Clients unterstützen automatische Knotenverweise für SMB.

Die Interoperabilitätsmatrix enthält die aktuellsten Informationen darüber, welche Windows Clients ONTAP unterstützt.

"NetApp Interoperabilitätsmatrix-Tool"

Anforderungen an Daten-LIFs

Wenn eine Daten-LIF als potenzielle Weiterleitung für SMB-Clients verwendet werden soll, müssen Daten-LIFs erstellt werden, bei denen sowohl NFS als auch CIFS aktiviert sind.

Automatische Knotenverweise können fehlschlagen, wenn der Zielknoten Daten-LIFs enthält, die nur für das NFS-Protokoll oder nur für das SMB-Protokoll aktiviert sind.

Wird diese Anforderung nicht erfüllt, ist der Datenzugriff nicht beeinträchtigt. Der SMB-Client ordnet die Freigabe mithilfe der ursprünglichen LIF zu, die der Client für die Verbindung zur SVM verwendet hat.

NTLM-Authentifizierungsanforderungen beim Herstellen einer weitergeleiteten SMB-Verbindung

NTLM-Authentifizierung muss in der Domäne, die den CIFS-Server enthält, sowie in den Domänen, die Clients enthalten, die automatische Knotenverweise nutzen möchten, erlaubt sein.

Bei einer Weiterleitung übermittelt der SMB-Server dem Windows-Client eine IP-Adresse. Da bei einer Verbindung über eine IP-Adresse die NTLM-Authentifizierung verwendet wird, findet für weitergeleitete Verbindungen keine Kerberos-Authentifizierung statt.

Dies geschieht, weil der Windows-Client den von Kerberos verwendeten Dienstprinzipalnamen (der die Form `service/NetBIOS name` und `service/FQDN` hat) nicht erstellen kann, was bedeutet, dass der Client kein Kerberos-Ticket für den Dienst anfordern kann.

Richtlinien für die Verwendung automatischer Knotenverweise mit der Home-Verzeichnis-Funktion

Wenn Freigaben mit aktivierter Home-Verzeichnis-Freigabeeigenschaft konfiguriert sind, können ein oder mehrere Home-Verzeichnis-Suchpfade für eine Home-Verzeichnis-Konfiguration eingerichtet werden. Die Suchpfade können auf Volumes verweisen, die sich auf jedem Knoten mit SVM-Volumes befinden. Clients erhalten eine Weiterleitung und stellen, sofern ein aktiver, lokaler Daten-LIF verfügbar ist, eine Verbindung über einen weitergeleiteten LIF her, der lokal zum Home-Verzeichnis des Benutzers ist.

Es gibt Richtlinien, wenn SMB 1.0-Clients auf dynamische Home-Verzeichnisse mit aktivierter automatischer Knotenweiterleitung zugreifen. Dies liegt daran, dass SMB 1.0-Clients die automatische Knotenweiterleitung benötigen, bevor sie sich authentifiziert haben, also bevor der SMB-Server den Benutzernamen kennt. Der Zugriff auf das SMB-Home-Verzeichnis funktioniert jedoch für SMB 1.0-Clients korrekt, wenn die folgenden Bedingungen erfüllt sind:

- SMB-Home-Verzeichnisse sind so konfiguriert, dass sie einfache Namen wie “%w” (Windows-Benutzername) oder “%u” (zugeordneter UNIX-Benutzername) verwenden und keine Namen im Domänenname-Stil wie "`%d\%w `" (Domänenname\Benutzername).
- Beim Erstellen von Home-Verzeichnisfreigaben werden die Namen der CIFS-Home-Verzeichnisfreigaben mit Variablen (“%w” oder “%u”) und nicht mit statischen Namen wie “HOME” konfiguriert.

Für SMB 2.x und SMB 3.0 Clients bestehen keine besonderen Richtlinien beim Zugriff auf Home-Verzeichnisse mit automatischen Knotenverweisen.

Richtlinien zum Deaktivieren automatischer Knotenverweise auf CIFS-Servern mit bestehenden weitergeleiteten Verbindungen

Wenn automatische Knotenverweise deaktiviert werden, nachdem die Option aktiviert wurde, behalten Clients, die aktuell mit einem verwiesenen LIF verbunden sind, die verwiesene Verbindung bei. Da ONTAP DFS-Verweise als Mechanismus für automatische SMB-Knotenverweise verwendet, können sich Clients sogar nach Deaktivierung der Option erneut mit dem verwiesenen LIF verbinden, bis der zwischengespeicherte DFS-Verweis des Clients für die verwiesene Verbindung abläuft. Dies gilt selbst im Fall einer Rückkehr zu einer Version von ONTAP, die automatische Knotenverweise nicht unterstützt. Clients verwenden weiterhin Verweise, bis der DFS-Verweis aus dem Cache des Clients abläuft.

Autolocation nutzt automatische Knotenverweise in SMB, um die Leistung von SMB-Clients zu steigern, indem Clients an den LIF auf dem Knoten weitergeleitet werden, der das Daten-Volume einer SVM besitzt. Wenn ein SMB-Client eine Verbindung zu einer auf einer SVM gehosteten SMB-Freigabe herstellt, kann die Verbindung über einen LIF auf einem Knoten erfolgen, der nicht die angeforderten Daten besitzt und das Cluster-Interconnect-Netzwerk zur Datenübertragung verwendet. Der Client kann von schnelleren Antwortzeiten profitieren, wenn die SMB-Verbindung einen LIF auf dem Knoten verwendet, der die angeforderten Daten enthält.

ONTAP stellt diese Funktionalität mithilfe von Microsoft Distributed File System (DFS) Verweisen bereit, um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein Ordner im Namespace an einem anderen Ort gehostet wird. Ein Node erstellt einen Verweis, wenn festgestellt wird, dass sich auf dem Node eine SVM LIF befindet, die die Daten enthält. Weiterleitungen erfolgen auf Grundlage des Speicherorts des Stammverzeichnisses der Freigabe, über die der Client verbunden ist.

Die Weiterleitung erfolgt während der SMB-Aushandlung. Die Weiterleitung erfolgt vor dem Verbindungsaufbau. Nachdem ONTAP den SMB-Client an den Zielknoten weitergeleitet hat, wird die Verbindung hergestellt und der Client greift ab diesem Zeitpunkt über den weitergeleiteten LIF-Pfad auf die Daten zu. Dies ermöglicht den Clients einen schnelleren Zugriff auf die Daten und vermeidet zusätzliche Cluster-Kommunikation.

Richtlinien für die Verwendung automatischer Knotenverweise mit Mac OS Clients

Mac OS X-Clients unterstützen keine automatischen SMB-Knotenverweise, obwohl Mac OS das Distributed File System (DFS) von Microsoft unterstützt. Windows-Clients stellen vor dem Verbinden mit einer SMB-Freigabe eine DFS-Verweisanfrage. ONTAP verweist auf eine Daten-LIF auf demselben Knoten, der die angeforderten Daten hostet, was zu verbesserten Antwortzeiten für die Clients führt. Obwohl Mac OS DFS unterstützt, verhalten sich Mac OS-Clients in diesem Bereich nicht exakt wie Windows-Clients.

Verwandte Informationen

- Informationen zur Aktivierung dynamischer Home-Verzeichnisse auf Servern
- "Netzwerkmanagement"
- "NetApp Interoperabilitätsmatrix-Tool"

Unterstützung für ONTAP SMB automatische Knotenweiterleitungen

Bevor Sie die automatischen Knotenverweise für SMB aktivieren, sollten Sie sich darüber im Klaren sein, dass bestimmte ONTAP Funktionalitäten keine Verweise unterstützen.

- Die folgenden Volume-Typen unterstützen keine automatischen Knotenverweise für SMB:
  - Schreibgeschützte Mitglieder eines Load-Sharing-Spiegels
  - Zielvolume eines Datensicherungsspiegels

- Knotenverweise werden bei einer LIF-Verschiebung nicht mitverschoben.

  Wenn ein Client eine referenzierte Verbindung über eine SMB 2.x oder SMB 3.0 Verbindung verwendet und ein Daten-LIF unterbrechungsfrei verschoben wird, verwendet der Client weiterhin dieselbe referenzierte Verbindung, auch wenn das LIF nicht mehr lokal zu den Daten ist.

- Knotenverweise werden nicht zusammen mit einer Volumenverschiebung verschoben.

  Wenn ein Client eine referenzierte Verbindung über eine beliebige SMB-Verbindung verwendet und eine Volume-Verschiebung erfolgt, verwendet der Client weiterhin dieselbe referenzierte Verbindung, auch wenn sich das Volume nicht mehr auf demselben Knoten wie die Daten-LIF befindet.

Automatische Knotenweiterleitungen für ONTAP SMB aktivieren oder deaktivieren

Die automatische Knotenweiterleitung für SMB kann aktiviert werden, um die Zugriffsleistung von SMB-Clients zu erhöhen. Die automatische Knotenweiterleitung kann deaktiviert werden, wenn keine Weiterleitungen von ONTAP an SMB-Clients erfolgen sollen.

Bevor Sie beginnen

Auf der Storage Virtual Machine (SVM) muss ein CIFS-Server konfiguriert und ausgeführt werden.

Über diese Aufgabe

Die automatische Knotenweiterleitungsfunktion von SMB ist standardmäßig deaktiviert. Diese Funktion kann bei Bedarf für jede SVM aktiviert oder deaktiviert werden.

Diese Option ist auf der Stufe „Erweitertes Berechtigungsniveau“ verfügbar.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. SMB automatische Knotenweiterleitungen nach Bedarf aktivieren oder deaktivieren:

Wenn Sie möchten, dass SMB automatische Knotenverweise…	Führen Sie den folgenden Befehl aus…
Aktiviert	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   Die Optionseinstellung wird für neue SMB-Sitzungen wirksam. Clients mit bestehender Verbindung können die Knotenweiterleitung nur verwenden, wenn ihre bestehende Cache-Zeitüberschreitung abgelaufen ist.

3. Zur Administratorberechtigungsstufe wechseln: `set -privilege admin`

Verwandte Informationen

Verfügbare Serveroptionen

Statistiken dienen zur Überwachung der automatischen Node-Referral-Aktivität von ONTAP SMB.

Um die Anzahl der weitergeleiteten SMB-Verbindungen zu ermitteln, kann die automatische Knotenweiterleitungsaktivität mithilfe des `statistics` Befehls überwacht werden. Durch die Überwachung der Weiterleitungen lässt sich feststellen, inwieweit automatische Weiterleitungen Verbindungen auf Knoten herstellen, die die Freigaben hosten, und ob eine Neuzuordnung der Daten-LIFs sinnvoll ist, um einen besseren lokalen Zugriff auf Freigaben auf dem CIFS-Server zu ermöglichen.

Über diese Aufgabe

Das `cifs`Objekt stellt auf der Ebene erweiterter Berechtigungen mehrere Zähler bereit, die bei der Überwachung automatischer Knotenverweise in SMB hilfreich sind:

- `node_referral_issued`

  Anzahl der Clients, die eine Weiterleitung zum Knoten des Share-Root erhalten haben, nachdem sich der Client über eine LIF verbunden hat, die von einem anderen Knoten als dem Share-Root-Knoten gehostet wird.

- `node_referral_local`

  Anzahl der Clients, die sich über einen LIF verbunden haben, der vom selben Knoten gehostet wird wie das Stammverzeichnis der Freigabe. Lokaler Zugriff bietet im Allgemeinen optimale Leistung.

- `node_referral_not_possible`

  Anzahl der Clients, denen nach der Verbindung über eine LIF, die von einem anderen Knoten als dem des Share-Root gehostet wird, keine Weiterleitung zum Knoten mit dem Share-Root zugewiesen wurde. Dies ist darauf zurückzuführen, dass keine aktive Daten-LIF für den Knoten mit dem Share-Root gefunden wurde.

- `node_referral_remote`

  Anzahl der Clients, die sich über eine LIF verbunden haben, die von einem anderen Knoten als dem Knoten, der das Stammverzeichnis der Freigabe hostet, gehostet wird. Remotezugriff kann zu einer verringerten Performance führen.

Sie können automatische Node-Referral-Statistiken auf Ihrer Storage Virtual Machine (SVM) überwachen, indem Sie Daten für einen bestimmten Zeitraum (eine Stichprobe) erfassen und anzeigen. Daten aus der Stichprobe können angezeigt werden, wenn die Datenerfassung nicht gestoppt wird. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird, besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Leistungstrends zu identifizieren.



Um die mit dem `statistics` Befehl gesammelten Informationen auszuwerten und zu nutzen, sollte die Verteilung der Clients in Ihren Umgebungen verstanden werden.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Automatische Knotenweiterleitungsstatistiken werden mit dem `statistics` Befehl angezeigt.

In diesem Beispiel werden automatische Node-Referral-Statistiken angezeigt, indem Daten für einen ausgewählten Zeitraum gesammelt und angezeigt werden:

a. Die Sammlung wird gestartet: `statistics start -object cifs -instance vs1 -sample -id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Warten, bis die gewünschte Erfassungszeit verstrichen ist.

c. Die Sammlung anhalten: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

d. Automatische Knotenverweis-Statistiken anzeigen: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                     Value
    -------------------------- --------------------------
    node_name                                   node1
    node_referral_issued                            0
    node_referral_local                             1
    node_referral_not_possible                      2
    node_referral_remote                            2
    ...

    node_name                                   node2
    node_referral_issued                            2
    node_referral_local                             1
    node_referral_not_possible                      0
    node_referral_remote                            2
    ...
```

Die Ausgabe zeigt Zähler für alle Knoten an, die an SVM vs1 teilnehmen. Zur besseren Übersicht werden im Beispiel nur Ausgabefelder bereitgestellt, die sich auf Statistiken zur automatischen Knotenzuweisung beziehen.

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

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

- Statistiken anzeigen
- "Einrichtung der Leistungsüberwachung"

Client-seitige ONTAP SMB-Informationen zur automatischen Knotenweiterleitung mit einem Windows-Client überwachen

Um festzustellen, welche Empfehlungen aus Sicht des Clients erfolgen, kann das Windows `dfsutil.exe` Dienstprogramm verwendet werden.

Das in Windows 7 und späteren Versionen enthaltene Remoteserver-Verwaltungstool (RSAT) enthält das `dfsutil.exe` Dienstprogramm. Mit diesem Dienstprogramm lassen sich Informationen zum Inhalt des Verweis-Caches sowie Informationen zu jedem Verweis anzeigen, den der Client aktuell verwendet. Das Dienstprogramm kann auch zum Leeren des Verweis-Caches des Clients verwendet werden. Weitere Informationen bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Ordnersicherheit auf Freigaben mit zugriffsbasierter Aufzählung bereitstellen

ONTAP SMB-Ordnersicherheit auf Freigaben mit zugriffsbasierter Aufzählung bereitstellen

Wenn die zugriffsbasierte Aufzählung (ABE) für eine SMB-Freigabe aktiviert ist, sehen Benutzer, die keine Berechtigung zum Zugriff auf einen in der Freigabe enthaltenen Ordner oder eine Datei haben (sei es aufgrund von individuellen oder Gruppenberechtigungsbeschränkungen), diese freigegebene Ressource in ihrer Umgebung nicht, obwohl die Freigabe selbst sichtbar bleibt.

Die herkömmlichen Freigabeeigenschaften ermöglichen es, festzulegen, welche Benutzer (einzeln oder in Gruppen) die Berechtigung haben, Dateien oder Ordner innerhalb der Freigabe anzuzeigen oder zu bearbeiten. Sie ermöglichen jedoch keine Kontrolle darüber, ob Ordner oder Dateien innerhalb der Freigabe für Benutzer sichtbar sind, die keine Zugriffsberechtigung haben. Dies könnte problematisch sein, wenn die Namen dieser Ordner oder Dateien innerhalb der Freigabe sensible Informationen beschreiben, wie beispielsweise die Namen von Kunden oder Produkten in der Entwicklung.

Die zugriffsbasierte Aufzählung (ABE) erweitert die Freigabeeigenschaften um die Auflistung der darin enthaltenen Dateien und Ordner. ABE ermöglicht daher, die Anzeige von Dateien und Ordnern innerhalb der Freigabe basierend auf den Benutzerzugriffsrechten zu filtern. Das bedeutet, die Freigabe selbst wäre für alle Benutzer sichtbar, aber Dateien und Ordner innerhalb der Freigabe könnten bestimmten Benutzern angezeigt oder vor ihnen verborgen werden. Zusätzlich zum Schutz sensibler Informationen am Arbeitsplatz ermöglicht ABE eine vereinfachte Darstellung großer Verzeichnisstrukturen für Benutzer, die keinen Zugriff auf den gesamten Inhalt benötigen. Beispielsweise wäre die Freigabe selbst für alle Benutzer sichtbar, aber Dateien und Ordner innerhalb der Freigabe könnten angezeigt oder verborgen werden.

Informationen dazu "Leistungsauswirkungen bei Verwendung der SMB/CIFS Access Based Enumeration".

Zugriffsbasierte Aufzählung für ONTAP SMB-Freigaben aktivieren oder deaktivieren

Sie können die zugriffsbasierte Aufzählung (ABE) auf SMB-Freigaben aktivieren oder deaktivieren, um zu erlauben oder zu verhindern, dass Benutzer freigegebene Ressourcen sehen, für die sie keine Zugriffsberechtigung haben.

Über diese Aufgabe

Standardmäßig ist ABE deaktiviert.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Geben Sie den Befehl ein…
ABE auf einer neuen Freigabe aktivieren	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration`Zusätzliche optionale Freigabeeinstellungen und weitere Freigabeeigenschaften lassen sich beim Erstellen einer SMB-Freigabe angeben. Weitere Informationen zu `vserver cifs share create` finden sich in der "ONTAP-Befehlsreferenz".
ABE für eine bestehende Freigabe aktivieren	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`Bestehende Share-Eigenschaften bleiben erhalten. Die ABE Share-Eigenschaft wird der bestehenden Liste der Share-Eigenschaften hinzugefügt.
ABE für eine bestehende Freigabe deaktivieren	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`Andere Freigabeeigenschaften bleiben erhalten. Nur die Freigabeeigenschaft ABE wird aus der Liste der Freigabeeigenschaften entfernt.

2. Es kann überprüft werden, ob die Freigabekonfiguration korrekt ist, indem der `vserver cifs share show` Befehl verwendet wird.

Beispiele

Das folgende Beispiel erstellt eine ABE-SMB-Freigabe mit dem Namen „sales“ und einem Pfad von `/sales` auf SVM vs1. Die Freigabe wird mit `access-based-enumeration` als Freigabeeigenschaft erstellt:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales
```

```
                    Vserver: vs1
                      Share: sales
     CIFS Server NetBIOS Name: VS1
                       Path: /sales
            Share Properties: access-based-enumeration
                              oplocks
                              browsable
                              changenotify
          Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
               Share Comment: -
                   Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Im folgenden Beispiel wird die `access-based-enumeration`Freigabeeigenschaft zu einer SMB-Freigabe mit dem Namen “data2” hinzugefügt:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Verwandte Informationen

Freigabeeigenschaften bei bestehenden Shares hinzufügen oder entfernen

Zugriffsbasierte Aufzählung von einem Windows-Client auf ONTAP SMB-Freigaben aktivieren oder deaktivieren

Der Zugriff auf die zugriffsbasierte Aufzählung (ABE) kann auf SMB-Freigaben von einem Windows-Client aus aktiviert oder deaktiviert werden, wodurch sich diese Freigabeeinstellung konfigurieren lässt, ohne dass eine Verbindung zum CIFS-Server erforderlich ist.

> Das `abecmd` Dienstprogramm ist in neueren Versionen von Windows Server und Windows Clients nicht verfügbar. Es wurde als Teil von Windows Server 2008 veröffentlicht. Der Support für Windows Server 2008 endete am 14. Januar 2020.

Schritte

1. Auf einem Windows-Client, der ABE unterstützt, wird folgender Befehl eingegeben: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Weitere Informationen zum `abecmd` Befehl sind in der Dokumentation Ihres Windows Clients zu finden.

Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen bei NFS und SMB

Informationen zu den Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen in ONTAP NFS und SMB

Die Namenskonventionen für Dateien und Verzeichnisse hängen sowohl von den Betriebssystemen der Netzwerkclients als auch von den Dateifreigabeprotokollen sowie von den Spracheinstellungen des ONTAP Clusters und der Clients ab.

Das Betriebssystem und die Dateiaustauschprotokolle bestimmen Folgendes:

- Zeichen, die ein Dateiname verwenden darf
- Groß-/Kleinschreibung eines Dateinamens

ONTAP unterstützt Mehrbytezeichen in Datei-, Verzeichnis- und Qtree-Namen, abhängig von der ONTAP Version.

Informationen zu gültigen Zeichen für ONTAP SMB Datei- oder Verzeichnisnamen

Wenn Sie von Clients mit unterschiedlichen Betriebssystemen auf eine Datei oder ein Verzeichnis zugreifen, empfiehlt sich die Verwendung von Zeichen, die in beiden Betriebssystemen gültig sind.

Wenn Sie beispielsweise unter UNIX eine Datei oder ein Verzeichnis erstellen, verwenden Sie keinen Doppelpunkt (:) im Namen, da der Doppelpunkt in MS-DOS-Datei- oder Verzeichnisnamen nicht zulässig ist. Da die Beschränkungen für zulässige Zeichen je nach Betriebssystem variieren, enthält die Dokumentation Ihres Client-Betriebssystems weitere Informationen zu verbotenen Zeichen.

Groß-/Kleinschreibung von ONTAP SMB Datei- und Verzeichnisnamen in einer Multiprotokollumgebung

Dateinamen und Verzeichnisnamen unterscheiden bei NFS-Clients zwischen Groß- und Kleinschreibung, bei SMB-Clients hingegen nicht, wobei die Groß-/Kleinschreibung erhalten bleibt. Es ist wichtig, die Auswirkungen in einer Multiprotokollumgebung zu kennen sowie die Maßnahmen, die beim Angeben des Pfads während der Erstellung von SMB-Freigaben und beim Zugriff auf Daten innerhalb der Freigaben erforderlich sein können.

Wenn ein SMB-Client ein Verzeichnis mit dem Namen `testdir` erstellt, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `testdir` an. Wenn jedoch ein SMB-Benutzer später versucht, ein Verzeichnis mit dem Namen `TESTDIR` zu erstellen, ist dies nicht zulässig, da dieser Name für den SMB-Client bereits existiert. Wenn ein NFS-Benutzer später ein Verzeichnis mit dem Namen `TESTDIR` erstellt, zeigen NFS- und SMB-Clients den Verzeichnisnamen unterschiedlich an, wie folgt:

- Auf NFS-Clients werden beide Verzeichnisnamen so angezeigt, wie sie erstellt wurden, zum Beispiel `testdir` und `TESTDIR`, da bei Verzeichnisnamen zwischen Groß- und Kleinschreibung unterschieden wird.
- SMB-Clients verwenden die 8.3-Namen, um die beiden Verzeichnisse zu unterscheiden. Ein Verzeichnis hat den Basisdateinamen. Weitere Verzeichnisse erhalten einen 8.3-Dateinamen.
  - Auf SMB-Clients sind `testdir` und `TESTDI~1` sichtbar.
  - ONTAP erstellt den `TESTDI~1` Verzeichnisnamen, um die beiden Verzeichnisse zu unterscheiden.

    In diesem Fall ist beim Angeben eines Freigabepfads beim Erstellen oder Ändern einer Freigabe auf einer Storage Virtual Machine (SVM) der 8.3-Name zu verwenden.

Ähnlich verhält es sich mit Dateien: Wenn ein SMB-Client `test.txt` erstellt, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `text.txt` an. Wenn jedoch ein SMB-Benutzer später versucht, `Test.txt` zu erstellen, ist dieser Name nicht zulässig, da er für den SMB-Client bereits existiert. Wenn ein NFS-Benutzer später eine Datei mit dem Namen `Test.txt` erstellt, zeigen NFS- und SMB-Clients den Dateinamen unterschiedlich an, wie folgt:

- Auf NFS-Clients werden beide Dateinamen so angezeigt, wie sie erstellt wurden, `test.txt` und `Test.txt`, da Dateinamen zwischen Groß- und Kleinschreibung unterscheiden.
- SMB-Clients verwenden die 8.3-Namen, um die beiden Dateien zu unterscheiden. Eine Datei hat den Basisdateinamen. Zusätzliche Dateien erhalten einen 8.3-Dateinamen.
  - Auf SMB-Clients sind `test.txt` und `TEST~1.TXT` sichtbar.
  - ONTAP erstellt den `TEST~1.TXT` Dateinamen, um die beiden Dateien zu unterscheiden.

> Wenn die Zeichenzuordnung mithilfe der Vserver CIFS-Zeichenzuordnungsbefehle aktiviert oder geändert wurde, wird eine normalerweise nicht zwischen Groß- und Kleinschreibung unterscheidende Windows-Suche zu einer Groß- und Kleinschreibung berücksichtigenden Suche.

Informationen zur Erstellung von ONTAP SMB Datei- und Verzeichnisnamen

ONTAP erstellt und verwaltet zwei Namen für Dateien oder Verzeichnisse in jedem Verzeichnis, auf das ein SMB-Client zugreifen kann: den ursprünglichen langen Namen und einen Namen im 8.3-Format.

Für Datei- oder Verzeichnisnamen, die die Grenze von acht Zeichen für den Namen oder die Grenze von drei Zeichen für die Dateierweiterung überschreiten, generiert ONTAP einen Namen im 8.3-Format wie folgt:

- Es kürzt den ursprünglichen Datei- oder Verzeichnisnamen auf sechs Zeichen, wenn der Name mehr als sechs Zeichen umfasst.
- Es hängt eine Tilde (~) und eine Zahl von eins bis fünf an Datei- oder Verzeichnisnamen an, die nach dem Kürzen nicht mehr eindeutig sind.

  Wenn keine weiteren Zahlen mehr verfügbar sind, weil es mehr als fünf ähnliche Namen gibt, wird ein eindeutiger Name erstellt, der keinerlei Bezug zum ursprünglichen Namen hat.
- Im Falle von Dateien wird die Dateinamenerweiterung auf drei Zeichen gekürzt.

Wenn ein NFS-Client beispielsweise eine Datei mit dem Namen `specifications.html` erstellt, ist der von

ONTAP im 8.3-Format generierte Dateiname `specif~1.htm`. Falls dieser Name bereits existiert, verwendet ONTAP eine andere Zahl am Ende des Dateinamens. Wenn ein NFS-Client anschließend eine weitere Datei mit dem Namen `specifications_new.html` erstellt, ist das 8.3-Format von `specifications_new.html` `specif~2.htm`.

Informationen zu ONTAP SMB Multibyte-Datei-, Verzeichnis- und Qtree-Namen

Ab ONTAP 9.5 ermöglicht die Unterstützung von 4-Byte-UTF-8-kodierten Namen die Erstellung und Anzeige von Datei-, Verzeichnis- und Baumnamen, die Unicode-Zusatzzeichen außerhalb der Basic Multilingual Plane (BMP) enthalten. In früheren Versionen wurden diese Zusatzzeichen in Multiprotokollumgebungen nicht korrekt angezeigt.

Um die Unterstützung für 4-Byte-UTF-8-kodierte Namen zu ermöglichen, steht für die `vserver` und `volume` Befehlsfamilien ein neuer Sprachcode *utf8mb4* zur Verfügung.

Sie müssen ein neues Volume auf eine der folgenden Arten erstellen:

- Die Option für das Volume `-language` explizit festlegen: `volume create -language utf8mb4 {…}`
- Übernahme der `-language` Volumenoption von einer SVM, die mit dieser Option erstellt oder für diese Option geändert wurde: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- In ONTAP 9.6 und früheren Versionen können bestehende Volumes nicht für die Unterstützung von utf8mb4 geändert werden; es ist erforderlich, ein neues utf8mb4-fähiges Volume zu erstellen und die Daten anschließend mithilfe clientbasierter Kopierwerkzeuge zu migrieren.

  SVMs können für die Unterstützung von utf8mb4 aktualisiert werden, bestehende Volumes behalten jedoch ihre ursprünglichen Sprachcodes.

  Wenn Sie ONTAP 9.7P1 oder höher verwenden, können bestehende Volumes für utf8mb4 mit einer Supportanfrage modifiziert werden. Weitere Informationen finden sich unter "Kann die Volume-Sprache nach der Erstellung in ONTAP geändert werden?".

- Ab ONTAP 9.8 kann der `[-language <Language code>]`Parameter verwendet werden, um die Volume-Sprache von *.UTF-8 auf utf8mb4 zu ändern. Für eine Änderung der Sprache eines Volumes ist "NetApp Support"zu kontaktieren.

> LUN-Namen mit 4-Byte-UTF-8-Zeichen werden derzeit nicht unterstützt.

- Unicode-Zeichendaten werden in Windows-Dateisystemanwendungen typischerweise mit dem 16-Bit-Unicode-Transformationsformat (UTF-16) und in NFS-Dateisystemen mit dem 8-Bit-Unicode-Transformationsformat (UTF-8) dargestellt.

  In Versionen vor ONTAP 9.5 wurden Namen mit UTF-16-Zusatzzeichen, die von Windows-Clients erstellt wurden, zwar anderen Windows-Clients korrekt angezeigt, jedoch nicht korrekt in UTF-8 für NFS-Clients übersetzt. Ebenso wurden Namen mit UTF-8-Zusatzzeichen, die von NFS-Clients erstellt wurden, nicht korrekt in UTF-16 für Windows-Clients übersetzt.

- Wenn auf Systemen, auf denen ONTAP 9.4 oder früher ausgeführt wird, Dateinamen erstellt werden, die gültige oder ungültige Zusatzzeichen enthalten, lehnt ONTAP den Dateinamen ab und gibt eine Fehlermeldung wegen eines ungültigen Dateinamens zurück.

Um dieses Problem zu vermeiden, sollten in Dateinamen ausschließlich BMP-Zeichen verwendet und auf die Verwendung von Zusatzzeichen verzichtet werden, oder es ist ein Upgrade auf ONTAP 9.5 oder höher durchzuführen.

Ab ONTAP 9 sind Unicode-Zeichen in qtree-Namen zulässig.

- Sie können entweder die `volume qtree` Befehlsfamilie oder den System Manager verwenden, um Qtree-Namen festzulegen oder zu ändern.
- Qtree Namen können Mehrbytezeichen im Unicode-Format enthalten, wie zum Beispiel japanische und chinesische Schriftzeichen.
- In Versionen vor ONTAP 9.5 wurden nur BMP-Zeichen (das heißt, solche, die in 3 Bytes dargestellt werden konnten) unterstützt.

> In Versionen vor ONTAP 9.5 kann der Verbindungspfad des übergeordneten Volumes eines Qtrees Qtree- und Verzeichnisnamen mit Unicode-Zeichen enthalten. Der `volume show` Befehl zeigt diese Namen korrekt an, wenn das übergeordnete Volume eine UTF-8-Spracheneinstellung hat. Wenn jedoch die Sprache des übergeordneten Volumes nicht zu den UTF-8-Spracheneinstellungen gehört, werden einige Teile des Verbindungspfads mit einem numerischen NFS-Alternativnamen angezeigt.

- In Version 9.5 und späteren Versionen werden 4-Byte-Zeichen in Qtree-Namen unterstützt, vorausgesetzt, der Qtree befindet sich in einem Volume, das für utf8mb4 aktiviert ist.

Zeichenzuordnung für die ONTAP SMB-Dateinamenübersetzung auf Volumes konfigurieren

NFS-Clients können Dateinamen erstellen, die Zeichen enthalten, die für SMB-Clients und bestimmte Windows-Anwendungen ungültig sind. Die Zeichenzuordnung für die Dateinamenübersetzung kann auf Volumes konfiguriert werden, sodass SMB-Clients auf Dateien mit NFS-Namen zugreifen können, die andernfalls ungültig wären.

Über diese Aufgabe

Wenn Dateien, die von NFS-Clients erstellt wurden, von SMB-Clients geöffnet werden, prüft ONTAP den Dateinamen. Ist der Name kein gültiger SMB-Dateiname (zum Beispiel wenn er einen eingebetteten Doppelpunkt ":" enthält), gibt ONTAP den 8.3-Dateinamen zurück, der für jede Datei gepflegt wird. Dies führt jedoch zu Problemen bei Anwendungen, die wichtige Informationen in langen Dateinamen codieren.

Wenn Sie also eine Datei zwischen Clients auf unterschiedlichen Betriebssystemen austauschen, sollten Sie in den Dateinamen Zeichen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie jedoch NFS-Clients haben, die Dateinamen mit Zeichen erstellen, die für SMB-Clients keine gültigen Dateinamen sind, kann eine Zuordnung definiert werden, die die ungültigen NFS-Zeichen in Unicode-Zeichen umwandelt, die sowohl von SMB als auch von bestimmten Windows-Anwendungen akzeptiert werden. Beispielsweise wird diese Funktionalität von den Anwendungen CATIA MCAD und Mathematica sowie anderen Anwendungen mit dieser Anforderung unterstützt.

Die Zeichenzuordnung kann für jedes Volume einzeln konfiguriert werden.

Bei der Konfiguration der Zeichenzuordnung auf einem Volume ist Folgendes zu beachten:

- Die Zeichenzuordnung wird nicht über Verbindungspunkte hinweg angewendet.

Die Zeichenzuordnung muss für jedes Verbindung Volume explizit konfiguriert werden.

- Sie müssen sicherstellen, dass die Unicode-Zeichen, die zur Darstellung ungültiger oder unzulässiger Zeichen verwendet werden, Zeichen sind, die normalerweise nicht in Dateinamen vorkommen; andernfalls treten unerwünschte Zuordnungen auf.

  Wenn Sie beispielsweise versuchen, einen Doppelpunkt (:) einem Bindestrich (-) zuzuordnen, der Bindestrich (-) aber im Dateinamen korrekt verwendet wurde, würde die Anfrage eines Windows-Clients, der auf eine Datei mit dem Namen “a-b” zugreifen möchte, dem NFS-Namen “a:b” zugeordnet (was nicht das gewünschte Ergebnis ist).

- Wenn nach der Anwendung der Zeichenzuordnung die Zuordnung immer noch ein ungültiges Windows-Zeichen enthält, greift ONTAP auf die Dateinamen von Windows 8.3 zurück.
- In FPolicy-Benachrichtigungen, NAS-Audit-Protokollen und Sicherheits-Trace-Meldungen werden die zugeordneten Dateinamen angezeigt.
- Wenn eine SnapMirror Relation vom Typ DP erstellt wird, wird die Zeichenzuordnung des Quellvolumes nicht auf das Zielvolume vom Typ DP repliziert.
- Groß-/Kleinschreibung: Da die zugeordneten Windows-Namen in NFS-Namen umgewandelt werden, folgt die Namensauflösung der NFS-Semantik. Das schließt ein, dass NFS-Suchen zwischen Groß- und Kleinschreibung unterscheiden. Das bedeutet, dass Anwendungen, die auf zugeordnete Freigaben zugreifen, sich nicht auf das Windows-Verhalten ohne Berücksichtigung der Groß- und Kleinschreibung verlassen dürfen. Der 8.3-Name ist jedoch verfügbar und unterscheidet nicht zwischen Groß- und Kleinschreibung.
- Unvollständige oder ungültige Zuordnungen: Nach der Zuordnung eines Namens zur Rückgabe an Clients, die eine Verzeichnisauflistung durchführen („dir“), wird der resultierende Unicode-Name auf Windows-Gültigkeit geprüft. Enthält dieser Name noch ungültige Zeichen oder ist er aus anderen Gründen für Windows ungültig (z. B. endet er mit einem Punkt oder ist leer), wird der 8.3 Name anstelle des ungültigen Namens zurückgegeben.

Schritt

1. Zeichenzuordnung konfigurieren: +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

Die Zuordnung besteht aus einer Liste von Quell-Ziel-Zeichenpaaren, die durch ":`" getrennt sind. Die Zeichen sind Unicode-Zeichen, die mit Hexadezimalziffern eingegeben werden. Beispiel: 3C:E03C. +

Der erste Wert jedes `mapping_text`Paars, das durch einen Doppelpunkt getrennt ist, ist der Hexadezimalwert des NFS-Zeichens, das Sie übersetzen möchten, und der zweite Wert ist der von SMB verwendete Unicode-Wert. Die Zuordnungspaare müssen eindeutig sein (eine Eins-zu-eins-Zuordnung sollte bestehen).

- Quellenzuordnung +

Die folgende Tabelle zeigt den zulässigen Unicode-Zeichensatz für die Quellzuordnung:

+

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x01-0x19	Nicht zutreffend	Nicht druckbare Steuerzeichen
0x5C		Backslash

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x3A	:	Doppelpunkt
0x2A	*	Sternchen
0x3F	?	Fragezeichen
0x22	"	Anführungszeichen
0x3C	<	Weniger als
0x3E	>	Größer als
0x7C		
Vertikale Linie	0xB1	±

- Zielzuordnung

  Sie können Zielzeichen im “Private Use Area” von Unicode im folgenden Bereich angeben: U+E0000… U+F8FF.

Beispiel

Der folgende Befehl erstellt eine Zeichenzuordnung für ein Volume mit dem Namen “data” auf der Storage Virtual Machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Verwandte Informationen

Informationen zum Erstellen und Verwalten von Datenvolumes in Namensräumen

ONTAP Befehle zur Verwaltung von Zeichenzuordnungen für die SMB-Dateinamenübersetzung

Sie können die Zeichenzuordnung verwalten, indem Sie Dateizeichenzuordnungen erstellen, ändern, Informationen darüber anzeigen oder löschen, die für die SMB-Dateinamenübersetzung auf FlexVol Volumes verwendet werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Neue Dateizeichenzuordnungen erstellen	`vserver cifs character-mapping create`
Informationen zu Dateizeichenzuordnungen	`vserver cifs character-mapping show`
Vorhandene Dateizeichenzuordnungen ändern	`vserver cifs character-mapping modify`
Dateizeichenzuordnungen löschen	`vserver cifs character-mapping delete`

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

Verwandte Informationen

Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren

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.